Australian Government

Department of Home Affairs

Protective Security Policy Framework

Australian Government Protective Security Policy Framework

Release 2024 | **Guidelines**

Contents

About the PSPF Guidelines

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 in domestically and internationally.

The PSPF Guidelines provide best practice advice to help Australian Government entities to implement the requirements of PSPF Release 2024.

The PSPF Guidelines are subordinate to the PSPF Release, and reference a number of Australian Government standards, frameworks and manuals.

See Figure 1 and PSPF Release 2024 for further information on the PSPF Structure and its elements.

Recommended Approaches

The PSPF requirements articulate what entities do to achieve desired protective security outcomes. The PSPF Requirements are detailed in PSPF Release 2024 and structured into their relevant protective security domain.

The PSPF Guidelines detail recommended approaches that represent best practice and are optional for entities to implement using a risk-based approach. Entities are not required to report on compliance with recommended approaches detailed in the PSPF Guidelines.

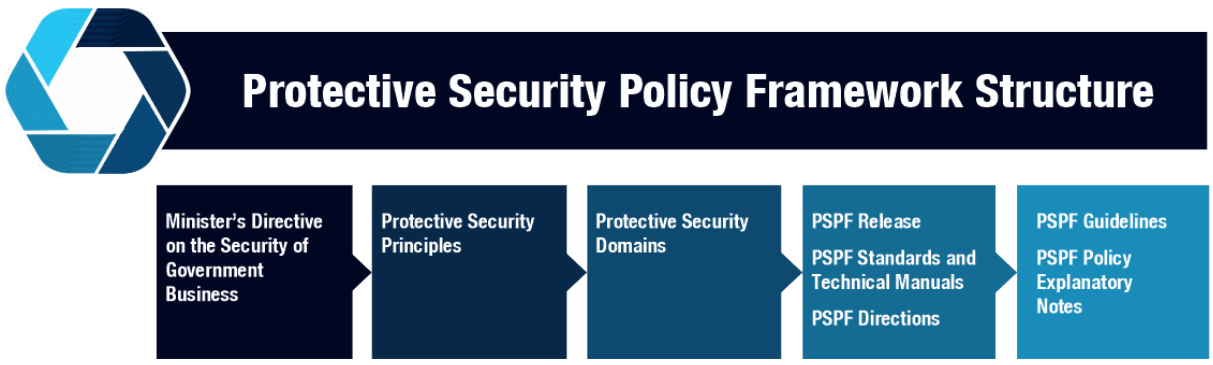
Contact Us

The Department of Home Affairs produces and maintains the PSPF and the PSPF Guidelines.

Contact:

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

Figure 1: PSPF Structure



Part One

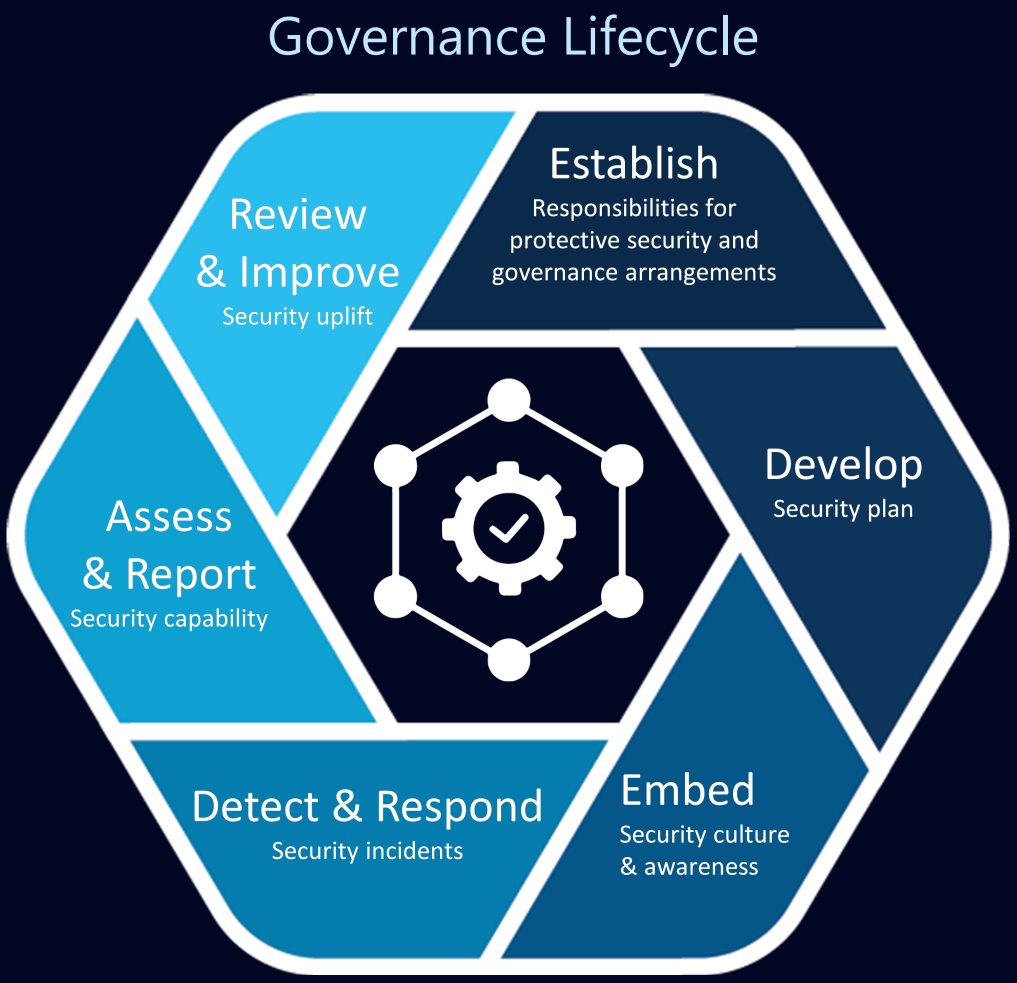
Governance

Whole-of-Government Protective Security Roles

Entity Protective Security Roles and Responsibilities

Security Planning, Incidents and Training

Protective Security Reporting



1 Whole-of-government Protective Security Roles

1.1 Departments of State

The Departments of State are the main bodies that reflect the structure of government. Departments of State also encompass the lead entity in each portfolio, as detailed in the Department of Finance's *List of Commonwealth Entities and Companies under the Public Governance, Performance and Accountability Act 2013 (PGPA Act)*.

Departments of State have additional protective security responsibilities. They are not required to be responsible for the security posture of portfolio entities. Rather, they are required to provide portfolio entities with timely security support and advice, when required, to assist them to achieve and maintain an acceptable level of security (appropriate to their risks) and remain aligned with government-wide security policies, priorities and plans. The Accountable Authority of the portfolio entity remains responsible for the security of their entity's people, information and resources.

1.1.1 Current Departments of State

At the date of publication, the Departments of State for the Australian Government are:

- Attorney-General's Department
- Department of Agriculture, Fisheries and Forestry
- Department of Climate Change, Energy, the Environment and Water
- Department of Defence
- Department of Education
- Department of Employment and Workplace Relations
- Department of Finance
- Department of Foreign Affairs and Trade
- Department of Health and Aged Care
- Department of Home Affairs
- Department of Industry, Science and Resources
- Department of Infrastructure, Transport, Regional Development, Communications and the Arts
- Department of the Prime Minister and Cabinet
- Department of Social Services
- Department of the Treasury
- Department of Veterans' Affairs

Recommended Approaches – Departments of State

- ✔ Implement appropriate oversight arrangements, including appointing an executive to coordinate security services to supported entities.
- ✔ Sustain capability to provide timely and accurate security advice and services.
- ✔ Maintain regular contact with the entities they support to increase awareness of the lead security entity's role and capabilities.

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.

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.

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.

The purpose of the Protective Security Direction (Direction) making power is to provide an intervention mechanisms to address specific security threats that present a significant risk to the Australian Government. Directions may be used to determine an entity's risk posture in relation to a specific threat or compel entities to adopt particular mitigations in response to a security threat.

PSPF Requirement 0002 mandates that Accountable Authorities of entities that are subject to the *Public Government, Performance and Accountability Act 2013* (PGPA Act) must adhere to any 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 Directions.

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

1.2.1.1. Types of Protective Security Directions

There are two types of Directions:

- Administrative Directions – Administrative Directions are issued to mitigate general security threats that present a significant risk to the Australian Government. Directed activities are likely to have resource impacts on entities, and therefore are expected to require implementation over a longer period of time.
- Emergency Directions - Emergency Directions are issued to mitigate a known or reasonably suspected security threat, vulnerability or incident that represents a significant risk to the Australian Government. Directed activities are likely to have short implementation timeframes, regardless of the resourcing impacts on entities.

1.2.1.2. Principles for Protective Security Directions

Directions will only be issued in accordance with the following guiding principles:

- the Direction addresses a significant security risk or opportunity to mitigate risk, to the Australian Government, or

- the Direction provides a proportionate, timely and flexible mechanism to align Australia with action taken by like-minded nations to address a significant security risk, or
- the Direction provides Accountable Authorities with the guidance required to allocate resources to assist the Department of Home Affairs to understand and address a systemic risk.

Directions will:

- detail the timeframe for compliance, noting entities must confirm compliance with each Direction in annual PSPF reporting, or provide an explanation of non-compliance, and
- where appropriate, be accompanied by a Policy Explanatory Note (PEN) which will provide further detail and implementation advice.

1.2.1.3. Consultation on Protective Security Directions

The Department of Home Affairs undertakes the following consultations arrangements to inform the Secretary of the Department of Home Affairs' decision to issue a proposed Direction.

- Government Security Committee (GSC) – provides Deputy Secretary-level (SES Band 3) strategic direction setting for whole-of-government protective security policy issues and challenges. The Deputy Secretary for Cyber and Infrastructure Security within the Department of Home Affairs chairs the GSC. See PSPF Release 2024 for further information on the GSC.
- Protective Security Board (PSB) – provides agency-head oversight of strategic protective security policy issues and challenges. The Secretary of the Department of Home Affairs chairs the PSB. See PSPF Release 2024 for further information on the PSB.
- Minister for Home Affairs, Minister for Immigration and Multicultural Affairs, and Minister for Cyber Security, and
- Relevant whole-of-government coordinators or authorities (e.g. National Cyber Security Coordinator, Counter Foreign Interference Coordinator, etc.).

1.2.1.4. Annual Review of Protective Security Directions

Directions are reviewed annually and either:

- incorporated into the following annual PSPF Release (each July) as mandatory requirements and then retired, or
- retired outright.

Direction 001-2023 on the TikTok application has been incorporated into PSPF Release 2024 and has therefore been retired. Directions 001-2024, 002-2024 and 003-2024, along with any future Directions issued prior to July 2025, will be reviewed as part of PSPF Release 2025.

1.2.2 Policy Explanatory Notes

Policy Explanatory Notes (PENs) provide advice and further information on specific security issues or topics that are not explicitly addressed in the PSPF, but there is an expectation that Australian Government entities are managing the risks.

PENs that are tied to a Direction are intended to help guide, define, and assist entities to meet their requirements and provide additional information to support consistent implementation of the Direction.

PENs that are not tied to a Direction are intended to provide entities with best practice or recommended actions to address specific security issues.

Where appropriate, the PEN will include a summary of the underlying risks that inform the need for the Direction. In cases where this information is PROTECTED, an OFFICIAL: Sensitive version of the PEN will be provided to entities without a PROTECTED GovLink email network.

1.3 Technical Authority Entities

The PSPF is supported by, and integrates, a number of technical manuals on specific security topics. These technical manuals take a variety of forms and may be a single manual, or a framework of advisory notes. Inclusion of those technical manuals into the PSPF denotes that they are also Australian Government policy.

Technical Authority Entities are those that have additional accountabilities to provide domain-specific security advice, technical standards or intelligence services in support of Australian Government protective security outcomes. Technical manuals, standards and advice are maintained by their respective Technical Authority Entity.

1.3.1 Current Technical Authority Entities

Table 1: Technical Authority Entities

Entity	Protective Security Responsibility
Attorney-General's Department (AGD)	Cybercrime and leadership for law enforcement policy.
Australian Federal Police (AFP)	Protective services for Australian high-office holders, foreign dignitaries, Commonwealth infrastructure, designated Commonwealth establishments and designated international airports, and diplomatic and consular missions in Australia.
Australian Secret Intelligence Service (ASIS)	Australia's overseas secret intelligence collection agency.
Australian Security Intelligence Organisation (ASIO)	Australia's national security intelligence service with investigative and advisory responsibilities including provision of threat assessments, protective and physical security services, and personnel security advice. ASIO prepares Technical Notes, Security Equipment Guides, and chairs the Security Construction and Equipment and Committee.
Australian Signals Directorate (ASD)	Australian Government cyber security technical controls and guidance, including the Australian Government Information Security Manual (ISM) and the Strategies to Mitigate Cyber Security Incidents, including the Essential Eight.
Department of Defence (Defence)	Security clearance vetting services to government and industry through the Australian Government Security Authorised Vetting Agency.
Department of Foreign Affairs and Trade (DFAT)	Whole-of-government security policy to protect Australian Government officials overseas.
Department of Home Affairs (Home Affairs)	Whole-of-government protective security policy to protect Australian Government people, information and resources. Prepares and administers the Australian Government Hosting Certification Framework and the Australian Government Gateway Policy. National Security Authority for international agreements and whole-of-government general security agreements.
Department of the Prime Minister and Cabinet (PM&C)	High-level leadership, direction and whole-of-government national security and intelligence policy coordination, and intergovernmental relations and communications with State and Territory Governments.

Entity	Protective Security Responsibility
National Archives of Australia (NAA)	Commonwealth records and information standards and advice.
Office of the Australian Information Commissioner (OAIC)	Whole-of-government information management policy and practice, including freedom of information and privacy.
Office of National Intelligence (ONI)	National Intelligence Community coordinator. Assessments and reports on international matters of political, strategic or economic significance to Australia, carrying out evaluations and otherwise advising the Prime Minister on matters relating to the intelligence community.

Recommended Approaches – Technical Advisory Entities

- Ensure the technical advice and guidance to support government entities to achieve and maintain and acceptable level of protective security is provided in a timely manner and through appropriate channels.
- Ensure technical standards, policy guidance and manuals remain aligned with the annual PSPF release.

1.4 Shared Service Provider Entities

Shared service provider entities provide corporate or technical services to other entities under an agreement or arrangement. Existing partnership and shared-service arrangements need to 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.

If the Accountable Authority of the shared service provider entity agrees, a supported entity may outsource responsibility for specific functions under shared-services or partnership arrangements. However, the Accountable Authority of the supported entity remains responsible for the overall security of their entity. For cross-portfolio arrangements, entities are encouraged to review reporting arrangements to their relevant ministers at regular intervals.

Recommended Approaches – Shared Service Provider Entities

- Establish clear responsibilities (agreed by all parties) including who will take lead control, and when.
- Establish arrangements for seeking technical or specialist advice to inform decisions about the shared arrangements.
- Establish escalation responsibilities (to whom and when), particularly if there are multiple ministers or governing bodies involved.
- Establish communication channels to maintain the flow of information between relevant parties (e.g. leadership, staff, contractors, building owners, in-house service providers) during an event or security incident.
- Apply a consistent approach, particularly for services to co-located entities.
- Schedule periodic reviews to consider the effectiveness of these arrangements and make procedural adjustments where necessary.

1.5 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.

Security vetting up to and including Positive Vetting can be conducted by:

- Australian Government Security Authorised Vetting Agency (AGSVA) are authorised to issue security clearances where the vetting assessment is sponsored by any Australian Government entity. AGSVA can issue security clearances up to and including the Positive Vetting level.
    - AGSVA is also authorised to issue security clearances for state and territory government agencies and other organisations 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 2006 Memorandum of Understanding for the Protection of National Security Information (available on GovTEAMS).
    - State and territory governments require an Australian Government entity to sponsor all Positive Vetting security clearances for their personnel.
- Other Authorised Vetting Agencies are authorised to issue security clearances for their own personnel. An Authorised Vetting Agency could have limitations on the level of security clearances it can issue, for example, some Authorised Vetting Agencies may only issue clearances at the Baseline level.

Security vetting for TOP SECRET-Privileged Access (TS-PA) security clearances can be conducted by:

- The TOP SECRET-Privileged Access Authority, authorised to implement requirements of the TOP SECRET-Privileged Access (TS-PA) Standard, issue TS-PA security clearances, and 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.
    - The TOP SECRET-Privileged Access Authority is also authorised to issue security clearances for state and territory government agencies and other organisations authorised by the Australian Government.

See PSPF Guidelines Section 18.1.118.1.1—Security Clearance Levels.

1.5.1 Current Authorised Vetting Agencies

Table 2 below lists the current Authorised Vetting Agencies for the Australian Government, as at the date of publication.

Table 2: Current Authorised Vetting Agencies

Authorised Vetting Agency	Security Clearance Level Authorised to Issue
Australian Federal Police (AFP)	Permitted to issue AFP clearances only, up to and including Negative Vetting 2
Australian Secret Intelligence Service (ASIS)	Permitted to issue ASIS security clearances only, up to and including Positive Vetting
Australian Securities and Investments Commission (ASIC)	Permitted to issue ASIC security clearances only, up to and including Baseline

Authorised Vetting Agency	Security Clearance Level Authorised to Issue
Australian Security Intelligence Organisation (ASIO)	Permitted to issue ASIO security clearances only, up to and including Negative Vetting 2
Australian Government Security Authorised Vetting Agency (Department of Defence)	Permitted to issue security clearances for the Australian Government1, up to and including Positive Vetting
Department of Foreign Affairs and Trade (DFAT)	Permitted to issue DFAT security clearances only, up to and including Positive Vetting
Office of National Intelligence (ONI)	Permitted to issue ONI security clearances only, up to and including Positive Vetting
TOP SECRET-Privileged Access Authority	Permitted to issue TOP SECRET-Privileged Access security clearances for the Australian Government[1]

1.5.2 Process to become an Authorised Vetting Agency for Baseline Clearances

The Government Security Committee (GSC) authorises Authorised Vetting Agencies on behalf of the Australian Government. Australian Government entities seeking authorisation to issue Australian Government Baseline security clearances for their own personnel, including contractors must:

- provide evidence that the entity meets the base eligibility criteria (available on request by emailing PSPF@homeaffairs.gov.au), including that the entity has fully implemented all PSPF personnel security requirements, and
- submit an application form approved by the entity's Chief Security Officer (or equivalent SES officer responsible for personnel security) to the Department of Home Affairs at PSPF@homeaffairs.gov.au for processing.

The application is then considered by the GSC, and if requested, the applying entity's Chief Security Officer (or other authorising SES officer) attends the GSC meeting. The applicant entity is advised of the outcome and any conditions imposed by GSC.

Once approved, the applicant entity must implement all PSPF requirements designated for AVAs in the next annual protective security reporting process.

1.6 Sponsoring Entities

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.

- Australian Government entities are authorised to sponsor Australian Government security clearances.
- State and territory government agencies are also authorised to sponsor security clearances.
- Organisations authorised by the Australian Government to sponsor security clearances.
    - This includes some Defence Industry Security Program (DISP) members who Department of Defence has authorised to sponsor Australian Government security clearances up to Negative Vetting 2. Contact disp.info@defence.gov.au for information on DISP.

[1] AGSVA and the TOP SECRET-Privileged Access Authority are also authorised to issue security clearance for state and territory government agencies and other organisations authorised by the Australian Government.

- Individuals or private organisations (other than those authorised by the Australian Government) are not eligible to sponsor an Australian Government security clearance.

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. A list of the Accountable Authority for each Commonwealth entity is listed in the Department of Finance's List of Commonwealth Entities and Companies under the PGPA Act.

Applicable sections of the PGPA Act:

- Section 12 Accountable Authorities – the Secretary of the Department or the person or group of persons, or governing body prescribed by an Act or the rules to be the Accountable Authority of the entity.
- Section 15 Duty to govern the Commonwealth entity: (1) The Accountable Authority of a Commonwealth entity must govern the entity in a way that: (a) promotes the proper use and management of public resources for which the authority is responsible.
- Section 21 Non-corporate Commonwealth entities (application of government policy) – The Accountable Authority of a Commonwealth entity must govern their entity in accordance with paragraph 15(1)(a) in a way that is not inconsistent with the policies of the Australian Government.

The Accountable Authority is answerable to their minister 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 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.

The Accountable Authority's role is to have effective protective security arrangements in place that achieve:

- compliance with PSPF requirements and standards
- capacity to function including during security incidents, disruptions or emergencies
- safety of those employed by the entity to carry out the functions of government (including contractors) and those who have dealings with the entity (including visitors), and
- protection of resources and information held within the entity.

2.1.1 Accountable Authority Protective Security Responsibilities

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.

See PSPF Guidelines Section 2.5—Security Governance.

Some PSPF requirements can only be completed by the Accountable Authority of the entity—that is the person or group of persons responsible for, and with control over, the entity's operations. Unless specified, these requirements cannot be delegated to another officer.

A summary of those responsibilities are listed below.

Table 3: Protective Security Responsibilities – Accountable Authority

Topic	Responsibility
Security culture	• Foster a positive security culture in the entity with clearly defined security expectations and priorities (PSPF Requirement 0023) • Provide security awareness training to all personnel (including contractors) to ensure they understand their security responsibilities (PSPF Requirement 0024 and PSPF Requirement 0025)
Security arrangements	• Implement the PSPF requirements and standards • Embed effective protective security arrangements that achieve: o capacity to function including during security incidents, disruptions or emergencies o safety of those employed by the entity to carry out the functions of government (including contractors) and those who have dealings with the entity (including visitors), and o protection of resources and information held within the entity
Security leadership	• Appoint and empower Chief Security Officer to be responsible for oversight of the entity's protective security arrangements • Appoint and empower a Chief Information Security Officer to provide cyber security leadership and support the Chief Security Officer
Adhere to Directions	• Adhere to any protective security directions issued by the Secretary of the Department of Home Affairs
Security plan	• Embed effective security risk management arrangements • Approve the entity's security plan and annual reviews to ensure the entity's security risks are appropriately managed
Report and monitor	• Verify and approve the entity's annual report on security as an accurate record of the entity's security posture • Establish proportionate monitoring arrangements to track security performance and plans to uplift areas of insufficient implementation
System authorisation	• Ensure all technology systems are assessed and authorised to operate by the appropriate authorising officer ensuring appropriate accreditation processes are

Topic	Responsibility
	in place for technology systems, including accepting any residual security risks to the system or the information the system processes, stores or communicates
Waivers	• Approve eligibility waiver requests (citizenship and uncheckable background)
Exceptional circumstances	• Confirm that any variances to mandatory PSPF requirements and standards due to exceptional circumstances are defendable, considered in light of the entity's risk tolerances, and are for a limited time period

2.2 Chief Security Officer

Chief Security Officers (CSOs) are the Australian Government's security custodians – they are key to ensuring the secure delivery of government business.

The 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 to assist the continuous delivery of business operations. Protective security practices are more likely to be effective when they are championed and demonstrated by senior management, embedded into entity operations and are well understood by all personnel.

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.

The CSO has the flexibility to delegate the day-to-day activities of protective security to security practitioners, although they retain responsibility for these activities. A key element of the CSO role is to ensure the entity and security practitioners have sufficient funding and resources allocated to achieve the protective security requirements the Government expects each entity to meet.

Success is ultimately tied to the work of the collective—it cannot be achieved in isolation. The CSO does not need to be an expert in all areas of protective security, rather, they require sufficient seniority, experience and judgement to make security-related decisions, drawing on the expertise of security practitioners to implement measures and strategies for each protective security requirement.

The scope and complexity of the CSO role depends on the nature of the entity's business and its risk environment. For smaller entities, it may be that the Accountable Authority takes on the role of the CSO and delegates the day-to-day functions of protective security to appointed security practitioners.

2.2.1 Chief Security Officer Responsibilities

Some PSPF requirements can only be completed by the CSO. Unless specified, these requirements cannot be delegated to another officer.

A summary of those responsibilities are listed below. See also Protective Security Guide for CSOs.

Table 4: Protective Security Responsibilities – Chief Security Officer

Topic	Responsibility
Security leadership	• Support the Accountable Authority to ensure the safety of personnel (including contractors, visitors and clients), information and resources. • Work closely with the CISO to ensure a consistent approach to protective security across the entity and to achieve the entity's security objectives.
Governance	• Form and chair a security governance committee, where required, to achieve oversight and support cohesion in protective security arrangements and decisions across the entity.
Strategic oversight	• Define the strategic direction and allocation of resources to deliver the security plan objectives, strengthen operations and improve the entity's security posture in order to make sound decisions about protective security planning. • Secure sufficient funding, resources and capability to implement PSPF requirements and protect the entity's people and resources.
Security practitioners	• Appoint sufficient security practitioners to perform specific security functions for the entity. • Create clear lines of reporting and accountability for personnel performing security-related functions, including those who do not report directly to the CSO.
Security arrangements	• Consolidate security arrangements across the entity, breaking down the silos that traditionally exist in security and leveraging the opportunities brought about by a holistic view of security. • Tailor security arrangements to the scale and complexity of the entity's operations and its risk environment.
Security culture and awareness	• Foster a positive security culture where personnel understand their responsibilities to manage security risk. • Embed efficient and effective security management awareness and practices by setting the strategic direction for protective security planning and risk management. • Ensure information and security awareness training programs are in place so personnel (including personnel and contractors located or travelling overseas) understand their security obligations.
Security planning	• Maintain an accurate and current security plan to managing the entity's security risks and drive improvements to address areas of vulnerability or low compliance.
Security procedures	• Establish effective procedures to achieve security outcomes that are consistent with the PSPF and other Australian Government policies and legal requirements.
Performance measures	• Establish security performance measures to monitor procedures to achieve required protections, address risks, counter unacceptable security risks, and improve security maturity.
Security incidents and investigations	• Manage the entity's response to security-related crises, incidents and emergencies in accordance with the entity's security incident and investigation procedures, and establish monitoring mechanisms across the entity.
Information sharing	• Disseminate and manage intelligence and threat information to stakeholders across the entity.
PSPF reporting	• Manage decision to deviate from the PSPF or implement alternative mitigations. • Oversee preparation of the entity's PSPF annual security report to accurately reflect its security position and compliance with the PSPF requirements, and detail how their entity is addressing areas of vulnerability.

Recommended Approaches

- The CSO is an appropriate level of seniority in the entity to achieve the protective security oversight functions, foster a positive security culture and drive improvements in protective security practice.
- The CSO has sufficient experience or be trained to perform the required security leadership and oversight functions.
- The CSO secures sufficient funding and resources to ensure the protection of the entity's people, information and resources.
- The CSO chairs the entity's security governance committee (if established), or otherwise holds membership on relevant internal committees.

2.3 Chief Information Security Officer

The Chief Information Security Officer (CISO) is responsible for providing cyber security leadership for the entity, incorporating information technology and operational technology. This includes responsibility for the entity's cyber security strategy and uplift plan and implementing ASD's ISM and Strategies to mitigate cyber security incidents.

The CISO is answerable to the Accountability Authority. The Accountable Authority determines the level of seniority required for the CISO role and who the CISO reports to. Where 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. This does not mean the CISO needs to report to the Accountable Authority but rather have line of sight to maintain accountability for cyber security leadership.

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.

PSPF Requirement 0012 mandates that the CISO must have the appropriate capability and experience to perform the CISO role. The CISO role is not Australian Public Service (APS) level specific but the appointed person needs to possess the appropriate capability, leadership experience and technical skills to perform the role and make informed cyber security decisions for the entity. The CISO adopts a continuous approach to learning and up-skilling in order to maintain pace with the cyber threat landscape and new technologies. See ASD's Guidelines for Cyber Security Roles for guidance.

2.3.1 Chief Information Security Officer Responsibilities

Some PSPF requirements are required to be completed by the CISO. Unless specified, these requirements cannot be delegated to another officer.

A summary of those responsibilities are listed below.

Table 5: Protective Security Responsibilities – Chief Information Security Officer

Topic	Responsibility
Security leadership	• Support the Accountable Authority by providing cyber security leadership • Reports to, or works closely with, the CSO to ensure a consistent approach to protective security across the entity and to achieve the entity's security objectives

Topic	Responsibility
Cyber security compliance	• Drive efforts to improve the entity's compliance with cyber security policy, standards, regulations and legislation – including: • Achieving the PSPF requirements • implementing the ISM's principles and controls • implementing ASD's Strategies to mitigate cyber security incidents • reviewing and updating the entity's cyber security program to ensure its relevance in addressing cyber threats and harnessing business and cyber security opportunities • Coordinating cyber security to ensure alignment of cyber security and the entity's business objectives
Cyber security practitioners	• Appoint sufficient cyber security practitioners (for example deputy CISOs or cyber security managers) to perform cyber security functions for the entity • Create clear lines of reporting and accountability for personnel performing cyber security-related functions, including those who do not report directly to the CISO
Manage systems and technology	• Manage the entity's systems and the data they process, store or communicate, including to ensure the security risks associated with the system's operation are acceptable before it is granted authorisation to operate by the relevant authority
Security incidents and investigations	• Ensure the entity's response to cyber-related crises, incidents and emergencies are in accordance with the entity's security incident and investigation procedures, PSPF requirements and related standards
PSPF reporting	• Contribute to the preparation of the entity's PSPF annual security report cyber security components to accurately reflect its security position and compliance with the PSPF requirements, and detail how they entity is addressing areas of vulnerability

Recommended Approaches

- The CISO is an appropriate level of seniority in the entity to perform the cyber security leadership functions of the role and make informed cyber security decisions for the entity.
- The CISO reports to the CSO, or otherwise works closely with the CSO to ensure a holistic approach to security is maintained.
- The CISO is an appropriate level of seniority in the entity to achieve the cyber security functions.
- The CISO holds a security clearance at the level commensurate with the entity's data holdings (with Negative Vetting 1 being the minimum as per PSPF Requirement 0012.
- The CISO holds membership on the security governance committee, if established within the entity.
- Cyber security practitioners report to a single senior officer, preferable the CISO, particular in larger entities, complex entities, or entities that carry high-risk and require multiple cyber security practitioners to manage cyber security-related functions.

2.3.2 Relationship with Other Government Roles

The CSO and CISO should work closely with senior officers appointed to perform roles mandated in other Australian Government policies or under regulatory obligations; particularly where those roles intersect with security-related functions. If the entity has established a security governance committee, the CSO should also consider what, if any, of these roles should be represented on that committee to ensure cohesion across the entity's security-related or peripheral activities.

Other mandated roles that are likely to have intersections with security are:

- Chief Data Officers (CDOs) are accountable for their entity's enterprise-wide governance and use of data as an asset, as well as building data capabilities.
    - CDOs should work with other senior leaders in the entity (including the CSO and CISO) to ensure data security and protection. See the Department of Finance's Chief Data Officer Information Pack for further guidance on this role.
- Chief Risk Officers (CROs) are responsible for maintaining the risk management policy that links the entity's risk management framework to its strategic objective(s).
    - CROs should work closely with the Accountable Authority, CSO and CISO to identify, measure and evaluate all key current, emerging and future risks. See the Department of Finance's Commonwealth Chief Risk Officer's Guide 2020 for further guidance on this role.
- Chief Privacy Officers (CPOs)/Privacy Champions are senior officials that perform privacy functions for the entity, including promoting a culture of privacy within the agency that values and protects personal information, providing leadership on strategic privacy issues, approving the entity's privacy management plan and reporting to the Accountable Authority on privacy issues.
    - CPOs/Privacy Champions should work closely with the CSO and CISO on security-related privacy matters and compliance with the Privacy Act. See OAICs' Privacy Champion, Chief Privacy Officer and Privacy Officer Roles for further guidance on this role.

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.

Specific security practitioner roles and titles are not mandated under the PSPF, other than the CSO and CISO roles. This provides flexibility for the CSO to establish and scale security arrangements.

The decision on whether security practitioners are required and if so, the number of security practitioners and their functions, is the responsibility of the CSO, other than for cyber security practitioners who are the responsibility of the CISO. Ideally security practitioners should report directly to, or have access to, the CSO, or CISO for cyber security practitioners. The number of security practitioners required and the scope of their remit will depend on the entity's size, complexity of business, infrastructure and risk environment. Given the range and complexity of security functions, it may be appropriate to the entity's operations or size to appoint separate practitioners for each security domain.

The CSO and CISO are responsible for encouraging a collaborative approach between security practitioners to enable governance, information, personnel and physical security measures that are complementary, promote robust security practices and achieve the entity's security objectives.

2.4.1 Security Practitioner Functions

The suggested specific functions that security practitioners be appointed to perform are detailed below. The CSO or CISO may appoint security practitioners to perform other functions where appropriate.

Table 6: Protective Security Functions – Security Practitioners

Topic	Responsibility
Governance	• Preparing security reports for the CSO or security committees, and assisting with gathering information to meet annual security reporting obligations

Topic	Responsibility
	• Coordinating and conducting security reviews • Liaising with law enforcement and intelligence agencies, other emergency services, service providers, clients and stakeholders • Responding to and coordinating security incident arrangements and being accessible for personnel to discuss security issues or concerns • Managing simple security investigations and escalating complex investigations to the CSO • Promoting the security and risk culture where personnel value and protect government information and resources • Establishing networks and relationships to understand the entity's business functions and vulnerabilities
Risk	• Identifying and managing governance security risks • Ensuring security plans and procedures are effective in achieving specified security outcomes • Monitoring security systems that facilitate the entity's capacity to function and identify security risks • Providing advice on protective security and security risk management arrangements • Ensuring security requirements are considered in other entity plans such as business continuity, fraud control and awareness
Information	• Ensuring appropriate procedures are established (in accordance with the PSPF) for the handling and protective marking of information • Managing access to information • Contributing to personnel awareness of information security obligations around appropriate use of IT equipment and official information • Providing briefings and advice to entity personnel on information, including briefings to personnel located or travelling overseas
Technology	• Identifying and managing cyber security risks • Managing access to data and systems that process, store or communicate that data • Ensuring the entity's technology systems are protected against unauthorised access or compromise, and information in electronic form is stored, processed and communicated in accordance with the law, Australian Government policies, and the information security requirements detailed in the entity's security plan • Monitoring information security systems and managing cyber security contractors to ensure the continued delivery of secure services • Safeguarding information from cyber threats and ensuring robust technology systems • Responding to and managing cyber incidents • Coordinating and conducting cyber security reviews • Liaising with and managing cyber security contractors in the delivery of secure services including: o mobile devices o internet and email gateways o cloud-based services, and o data centres, data storage and recovery
Personnel	• Identifying and managing personnel security risks • Managing the entity's personnel security program • Developing and conducting security awareness training programs (including refresher and specialised training)

Topic	Responsibility
	• Managing eligibility and suitability of personnel procedures • Monitoring ongoing assessment of personnel • Coordinating the personnel security aftercare program for separation of personnel, including withdrawing accesses and informing about ongoing security obligations • Providing advice on personnel security, including briefings to personnel located or travelling overseas
Physical	• Identifying and managing physical security risks • Ensuring a safe and secure physical environment for entity personnel, contractors, clients and the public • Ensuring a secure physical environment for official resources • Managing physical security measures and access controls to protect facilities, information and physical assets, for example certification of security zones • Liaising with and managing security contractors in the delivery of security services, including: o Security Construction and Equipment Committee (SCEC) endorsed consultants o Security industry specialists o Security guards (guarding) o Safe hand and overnight couriers o Secure destruction o Locksmithing services, and o Strategic planning for preparation of new or green-field sites

2.4.2 Competencies, Skills and Knowledge

Where appointed, security practitioners should possess, or be given sufficient training to develop, competency in the relevant areas of protective security, noting that some functions of a security practitioner will involve specialised skills.

As a base, security practitioners should demonstrate comprehensive knowledge or technical competencies in:

- the PSPF and its subordinate standards, for example ASIO Technical Notes and ASD's ISM
- security risk management and risk assessment
- developing and delivering security awareness training and security briefings, and
- professional certifications for technical functions.

The knowledge, competencies and skills can be attained through on-the-job training, prior experience in a related field or formal qualifications (e.g. tertiary qualifications such as the Certificate IV, Diploma in Government Security or equivalent qualification).

Registered Training Organisations (RTOs) are accredited training providers that offer nationally recognised training courses. RTO accredited courses are preferred where entities provide training towards formal qualifications for security practitioners. A list of these organisations is available from www.training.gov.au.

The CSO or CISO retain responsibility for security even if they elect to use contractors to perform specific security functions, including where professional technical certification is required (e.g. SCEC security zone consultants for Type 1a security alarm system compliance and IRAP Assessors for technology systems). This responsibility does not transfer to the contractor. These arrangements require monitoring to ensure the contracted provider fulfils the obligations of the PSPF and any entity-specific requirements.

2.5 Security Governance

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

Regardless of the structure implemented, the Accountable Authority and CSO retain overarching responsibility for protective security.

Good security governance:

- Provides a holistic, cohesive and coordinated strategic approach to security managing and planning.
- Appoints and empowers appropriately skilled and resourced personnel to achieve security outcomes.
- Establishes clear lines of reporting and accountability for security-related functions
- Implements fit-for-purpose security procedures that achieve the required security outcomes.
- Monitors the effectiveness of security management and compliance with the PSPF requirements and standards.
- Fosters a positive security culture and embeds effective security practices and training.
- Establishes protective security goals and strategic objectives.
- Monitors security plans and contributes to the annual review of the plan.
- Identifies and manages security risks both known and emerging.
- Considers outcomes of security incidents and investigations.
- Facilitates information sharing for security improvements.
- Seeks advice and briefings to keep across the threat environment.

2.5.1 Security Governance Committee

Establishing and chairing a security governance committee is one way the CSO can achieve and maintain the required level of protective security oversight and accountability across all areas of security for the entity.

While it is not mandatory to have a security governance committee, it may be a useful approach for entities that are large, high-risk, complex or dependent on other entities for protective security functions.

2.5.2 Security Email Address

The siloing of security information in an entity can inhibit effective security management. Silos may be the result of a number of behavioural or systemic problems, including something as simple as email management.

To address this, PSPF Requirement 0020 mandates a monitored email address for security-related matters to protect against information loss during times of change in security personnel and to facilitate the flow of security-related information. This email is recommended to be generic in nature and accessible by all relevant security parties.

2.5.2.1. Distribution of PSPF-Related Information

All PSPF-related information, advice and supporting materials will be distributed to the appointed CSO (or CISO for cyber security matters) and the entity's generic security email. CSOs, and where known, the CISOs, are blind copied (BCC) into these emails to protect their identity and reduce the need to raise the classification of the email. Alternatively, a separate email will be sent to CSOs and CISOs.

The Department of Home Affairs maintains a list of all CSOs, CISOs (where advised) and nominated generic security email addresses. Where the entity is unable to provide a generic email address for security-related matters and relies on an individual's email address, entities are encouraged to ensure the flow of security information is maintained during periods of absence, or if the person that owns the email address leaves that position. For example, the individual's email nominated for security-related matters is monitored by another officer, or is accessible to other officers who perform security functions.

This requirement does not preclude entities from maintaining other security-related mailboxes (e.g. to limit information based on the need-to-know or for sensitive matters). However, the main monitored email address will be used for all PSPF related correspondence unless otherwise advised.

Government personnel who have a need to receive PSPF-related information, advice and supporting materials should contact the person or team responsible for managing their entity's nominated generic security email address and ask to be added to the distribution list, rather than contacting the Department of Home Affairs.

Recommended Approaches

- Sufficient security practitioner positions are in place to perform security functions to support the continuous delivery of the entity's business operations.
- Each security practitioner position has clearly defined responsibilities with sufficient authority to perform those responsibilities and achieve the entity's security objectives.
- Security practitioners work together to ensure consistent approach to protective security, maintain appropriate visibility over entity security operations and decisions, and have regular access to the entity's CSO and/or CISO.
- Security practitioners attend relevant industry conferences, training and events to ensure their knowledge and skills keep pace with change.
- The CSO is the Chair of the Security Governance Committee (if established in the entity).
- The CISO is a member of the Security Governance Committee (if established in the entity).
- The Security Governance Committee meets on a regular basis to monitor all areas of security and support informed decisions on security arrangements for the entity, and provides the Accountable Authority with regular reports on the status of the entity's security posture and compliance position.
- The generic security email address takes the form security@[entityname].gov.au or pspf@[entityname].gov.au
- The generic security email is monitored to ensure the flow of security-related information to the Accountable Authority, CSO, CISO, security practitioners, security governance committee members and other relevant areas in the entity.
- The entity advises the Department of Home Affairs of any changes in CSO, CISO or generic security email address to PSPF@homeaffairs.gov.au

3 Security Planning, Incidents and Training

3.1 Security Planning

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.

Entities are encouraged to use security planning approaches that manage risks for the Australian Government and best meet their operational environment.

3.1.1 Security Plan Responsibilities

Security is everyone's responsibility, however, overall accountability for security planning and risk management rests with the entity's Accountable Authority, supported by the CSO, and the CISO for cyber security.

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 protective security planning. The security plan also specifies the responsibilities and resources applied to managing protective security risks. The security plan allows entities to review the degree of security risk that exists in different areas of operations and take action to mitigate identified risks.

The CSO can delegate development of the security plan to the person or persons that have an understanding of the entity's strategic goals and objectives and possesses the appropriate level of security risk management knowledge and expertise. However, this does not obviate the obligation to be responsible for the security plan and, where required, any supporting plans.

PSPF Requirement 0019 specifies that the Accountable Authority must approve the entity's security plan.

Recommended Approaches

- A single security plan, or an overarching security plan where impracticable due to the entity's size or complexity, is approved by the Accountable Authority.
- Supporting security plans (where required) are approved by the CSO or CISO (for cyber security plans), or their delegate.
- Entities liaise with other internal corporate areas (for example human resources, business continuity, property and procurement) to ensure an embedded approach, to understand the strategic direction of these areas and to identify any potential impacts on security planning.

3.1.2 Security Planning Approach

Successfully managing entity security risks and protecting people, information and resources requires an understanding of what needs protecting, what the threat is and how assets will be protected. Security planning is designing, implementing, monitoring, reviewing and continually improving practices for security risk management.

- Security plan (see Developing a Security Plan) – specifies the approach, responsibilities and resources applied to managing protective security risks. The security plan allows entities to review

the degree of security risk that exists in different areas of operations and take action to mitigate identified risks.

- Security risk management process (see Security Risk Management) – manages risks across all areas of security (governance, risk, information, technology, personnel and physical) to determine sources of threat and risk (and potential events) that could affect government or entity business. Security risk management includes:
    - security risk assessments, which are structured and comprehensive processes to identify, analyse and evaluate security risks and determine practical steps to minimise the risks
    - security risk treatments, which are the considered, coordinated and efficient actions and resources required to mitigate or lessen the likelihood or negative consequences of risks.

Regardless of an entity's functions or security concerns, the central messages for managing security risks are:

- security is everyone's responsibility and risk management is the business of all personnel (including contractors) in the entity, supported by security awareness training
- security is a business enabler that informs decision-making, is part of day-to-day business and is embedded into an entity's business processes
- security management is logical, systematic and transparent and is part of the enterprise risk management process, and
- security processes identify changes in the threat environment and allow for adjustments to maintain acceptable levels of risk, balancing operational and security needs.

3.1.2.1. Security Planning for Projects

Security should be considered during all stages of project management and planning. This is particularly important for projects that involve:

- major acquisitions
- establishment of infrastructure or major modifications to existing infrastructure, or
- information that is:
    - sensitive in nature or security classified
    - proprietary in nature, or
    - meets the financial and economic impact threshold with a business impact of low to medium (level two) or higher.

3.1.3 Developing a Security Plan

PSPF Requirement 0018 mandates that a security plan is developed, implemented and maintained to address the mandatory elements of the plan.

A security plan articulates how security risks are managed in the entity and how security aligns with other priorities and objectives. The security plan reflects the entity's protective security requirements and mitigation strategies appropriate to the levels of threat, risks to its assets and risk tolerances.

Entities are encouraged to make the security plan (and supporting security plans) available across the entity, particularly for those with obligations or responsibilities identified in the plan, as this helps to build a positive security culture based on a common understanding of security.

When developing or reviewing the security plan (and supporting security plans), entities are encouraged to seek advice and technical assistance from specialist entities such as:

- Australian Security Intelligence Organisation for threat assessments
- ASIO-T4 Protective Security for physical security advice or technical assistance
- local police for state and territory criminal threat information
- Australian Government Security Authorised Vetting Agency for security vetting procedural advice
- ASD for IT, cyber security and certified cloud services advice, and
- subject-matter experts.

Table 7 Suggested Coverage for Security Plan

Domain	Suggested Coverage
Governance	• Roles and responsibilities • Security incidents • Security culture • Security awareness training • Security monitoring • Reporting security maturity
Risk	• Risk tolerances • Security risk management (including threat, vulnerability and criticality assessments) • Contracted service providers
Information	• Classification and management arrangements for information holdings • Access to information including sharing information • Information management record keeping systems
Technology	• Technology access and system security • Cyber security to mitigate targeted intrusions • Information handling within the entity as well as when in transit or out of the office
Personnel	• Personnel security provisions during recruitment in conjunction with human resource management • Security clearance maintenance plans that address risks identified by security Authorised Vetting Agencies • Security assessment position list • Contact reporting • Security clearance aftercare • Ongoing security awareness training • Managing the separation of personnel
Physical	• Access control systems • Security monitoring and alarm systems • Measures to increase security if the National Terrorism Alert Level or entity-specific threats increase

Recommended Approaches

- ✔ Security plans are comprehensive and span all areas of protective security.
- ✔ Security plans are informed by expert or technical advice (where required).

PSPF Release 2024 (Table 1) details the mandatory elements of the security plan.

3.1.3.1. Element: Security Goals and Objectives

PSPF Release 2024 mandates that 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 as reflected in the entity's corporate plan. Security is everyone's responsibility, however overall accountability for security planning and risk management should rest with the entity's Accountable Authority, supported by the CSO.

Clear protective security goals and strategic objectives allow effective implementation of security risk management that is consistent with the entity's operating objectives. This will include the entity's commitment to security risk management, expectations for a positive security and risk culture, and the entity's security goals and strategic objectives.

Security goals are broader, longer-term, achievable outcomes relating to protective security. Strategic objectives are more tangible, shorter-term, specific deliverables relating to protective security.

Consider:

- vigilance, resilience and adaptability of personnel to security risks
- capacity to function, including during security incidents, disruptions or emergencies
- safety of personnel (including contractors) and those who have dealings with government (including visitors), and
- protection of information, resources, assets and facilities held in the entity.

Recommended Approaches

- When setting goals, consider the historical experience and knowledge results from previous performance indicators and past compliance with the PSPF.
- Entities assess their existing protective security arrangements and procedures to identify areas for improvement. This could be areas of exposure, vulnerability or 'target attractiveness'. Target attractiveness is the value of an entity or its components to an adversary when viewed as a target.
- Reviewing protective security arrangements should also consider the entity's compliance with implementing PSPF requirements.

3.1.3.2. Element: Security Risk Environment

PSPF Release 2024 mandates that 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, including:

- identify the people, information, and resources to be safeguarded
- determine specific risks (including shared risks) to the entity's people, information and resources in Australia and abroad (risk identification)
- identify the threats to people, information and resources (threat assessment)
- assess the degree of susceptibility and resilience to hazards (vulnerability assessment)
- assess the likelihood and consequence of each risk occurring (risk analysis)
- determine adequacy of existing safeguards and whether current risks (or residual vulnerabilities) are acceptable or not (evaluate risks)

- implement protective security measures to mitigate or reduce identified risks to an acceptable level (risk treatments)
- manage residual risks (treatable and untreatable) and vulnerabilities, and
- identify and accept responsibility for risks.

See PSPF Guidelines Chapter 5 for further guidance on the Security Risk Management Process and Section 3.1.3.9 for Critical People and Resources.

Recommended Approach

- Adopt a security risk management approach that is compatible with security requirements, the entity's risk profile and aligns with the relevant risk management standards, such as:
  - Department of Finance's Commonwealth Risk Management Policy
  - Australian Standards AS/NZS ISO 31000 Risk Management – Guidelines and HB 167 – Security Risk Management.

3.1.3.3. Element: Risk Tolerance

PSPF Release 2024 mandates that the security plan must detail the entity's tolerance to security risks, agreed by the Accountable Authority. 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.

See PSPF Guidelines Section 5.1 for further guidance on Security Risk Tolerance.

3.1.3.4. Element: Security Capability

PSPF Release 2024 mandates that the security plan must detail the entity's capability to manage security risks.

Security capability refers to an entity's security position in relation to its specific risk environment and risk tolerances. This includes acknowledging the successes and effectiveness of PSPF implementation, as well as highlighting areas for improvement.

Security capability considers how holistically and effectively each entity:

- implements and meets the intent of the PSPF requirements
- minimises harm to the government's people information and resources
- fosters a positive security culture
- responds to and learns from security incidents
- understands and manages its security risks, and
- achieves security outcomes while delivering business objectives.

3.1.3.5. Element: Security Risk Management Strategies

PSPF Release 2024 mandates that the security plan must detail the entity's mitigation strategies appropriate to the levels of threat, risks to its assets and risk tolerances, and strategies to implement security risk management and maintain a positive risk culture.

The entity's approach to managing security risks is critical, 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 assets. This includes:

- establishing risk stewards and managers
- instigating steps that minimise risks (according to risk environment and tolerances), and
- managing residual risks to ensure the protection of people, information and resources.

3.1.3.6. Element: Implications of Risk Decisions

PSPF Release 2024 mandates that 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.

PSPF Requirement 0038 mandates that 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.

- Particular consideration is required where a Department of State's decision has adverse implications for a supported entity. The supported entity may have a different risk tolerance level or limited capacity to meet the resulting obligations.
- Entities are strongly encouraged to adopt a default position to seek and share information (unless security, secrecy or privacy limitations are in place). In the event these limitations are in place, entities are encouraged to look at options that allow partial sharing of information.
- Where there are legislative limitations, such as under the *Privacy Act 1988*, entities may consider using formal agreements with other entities to share information.
- Sharing information between entities may help to mitigate threats across government. For example, parties that pose security threats, such as organised crime groups, may target multiple government entities.

3.1.3.7. Element: PSPF Implementation

PSPF Release 2024 mandates that the security plan must detail how the entity will implement the requirements of the PSPF.

PSPF Requirements are mandatory and must be fully implemented. Implementation involves deciding on the resources required to ensure the requirement is met, and ongoing resources needed to maintain the required level of protective security and identifies resources that may be needed to take additional precautions if the threat level increases.

PSPF Requirements that are designated as 'compliance' may be implemented using a 'risk managed' approach provided the entity provides a summary of what prevented full implementation of the requirement and a risk management plan detailing the arrangements for managing the requirement. The risk managed category is not intended to be enduring or long term, but rather allows the entity to put in place proportional mitigation arrangements until such time as the requirement can be fully implemented.

See PSPF Guidelines Section 4.2.2.1 for further information on the annual protective security reporting process.

3.1.3.8. Element: PSPF Directions

PSPF Release 2024 mandates that the security plan must detail the entity's approach to implementing the requirements specified in any Directions, including to ensure any timeframes or additional reporting obligations are met. If the Direction allows, the security plan must also detail the entity's arrangements to implement alternative mitigations to achieve the intent of the Direction.

See PSPF Guidelines Section 1.2.1 for further guidance on Protective Security Directions.

3.1.3.9. Element: Critical People and Resources

PSPF Release 2024 mandates that the security plan must identify people and resources that are critical to the ongoing operation of the entity and the national interest (criticality assessment), including:

- Resources that have a value to the entity and are relied on to sustain critical operations and capabilities.
    - Resources includes applications/technology systems/mobile devices that process, store or communicate official and security classified information/data, tangible assets (and their components), equipment, facilities, buildings and other spaces/places, elements of infrastructure and intangible assets such as data centres.
    - This should also capture any methodologies, classified military/intelligence activities or operations that are critical to the ongoing operation of the entity.
- People that are critical to sustaining the entity's ongoing operations and capabilities.
    - People includes employees, contractors, secondees and critical service providers.

It must detail the protections applied to safeguard these resources to support the continuity of the entity's core business.

3.1.3.10. Element: Threat Levels

PSPF Release 2024 mandates that the security plan must detail scalable control measures to meet increases or decreases in risk as a consequence of a change in threat to the entity. These must be able to accommodate changes in the National Terrorism Threat Level.

See **Table 8** for the business impact levels for consequences of threat levels.

Measures could include:

- determining who needs to know about changes in the security threat level
- outlining specific roles or responsibilities including who is responsible for determining the security alert level
- ensuring personnel are aware of the measures employed by the entity to adapt to and mitigate emergencies and heightened threat levels, and
- detailing arrangements to monitor the threat level and review the security alert level when the entity undertakes significant new projects, the risk environment changes, or after a significant incident impacting the entity's ability to operate.

Table 8: Business Impact Levels for Consequences of Threat

Business Impact Level	1 Low Impact	2 Low to Medium Impact	3 High Impact	4 Extreme Impact	5 Catastrophic Impact
Consequence of threat	Insignificant damage to the national interest, organisations or individuals.	Limited damage to the national interest, organisations or individuals.	Damage to the national interest, organisations or individuals.	Serious damage to the national interest, organisations or individuals.	Exceptionally grave damage to the national interest, organisations or individuals.

Developing entity security alert levels is one way an entity can ensure personnel are aware of the measures employed by the entity to adapt to and mitigate emergencies and heightened threat levels. Alert levels also allow entities to scale the controls used to mitigate risks as the risks increase or decrease.

The number of alert levels required for the entity will depend on its operational requirements and expected changes in risk sources. See Table 9 for examples of security alert levels.

The source of security risks can be categorised into three areas:

- **Event** – an event is an important happening or incident impacting on the entity's ability to function such as a natural event (e.g. storm) or an emergency event (e.g. fire).
- **Threat** – a threat is a declared intent to inflict harm on entity personnel or property.
- **Activity** – an activity is an action by one or more people likely to have a negative impact on physical security (e.g. protest activity, filming in the vicinity of premises).

Table 9: Examples of Security Alert Levels

Security Alert Levels	Low	Medium	High	Extreme	Catastrophic
Likelihood of threat	Applies when only general concerns exist of an event, physical activity or general threat.	Applies when an event, physical activity or threat is assessed as feasible.	Applies when an event, physical activity or threat is likely to occur.	Applies when an event, physical activity or threat is imminent or has occurred.	Applies when a severe event, physical activity or threat is imminent or has occurred.
Security measures required	Existing security measures are sufficient.	Security measures are maintainable indefinitely, with minimal impact to the entity's operations.	Security measures are sustainable for lengthy periods without causing undue hardship to personnel, affecting operational capability or aggravating relationships with the local community.	Security measures will not be sustainable over the long term without creating hardship and affecting the entity's activities and personnel.	Advice required from the National Security Hotline on additional security measures.

When determining the security alert level, entities are encouraged to monitor:

- National Terrorism Threat Level Advisory System advice
- protective security risk reviews
- police advice
- emergency management advice
- Bureau of Meteorology advice
- entity security incident reports, and
- media reports.

3.1.3.11. Element: Incident Management Plan

PSPF Release 2024 mandates that the security plan must detail must detail entity's security incident management plan covering the procedures to ensure security incidents are identified, managed and responded to.

PSPF Requirement 0026 mandates that procedures are developed, implemented and maintained to ensure security incidents are managed and responded to.

See PSPF Guidelines Section 3.6.3 for further guidance on managing security incidents.
See Cyber Security Incident Response Planning: Practitioner Guidance | Cyber.gov.au for guidance on developing a cyber incident response plan.

3.1.3.12. Element: Monitoring and Improvement

PSPF Release 2024 mandates that the security plan must detail the entity's monitoring arrangements and plans to uplift protective security improvement in areas of insufficient implementation.

See PSPF Guidelines Section 3.3—Continuous Monitoring and Improvement

3.1.3.13. Element: Review

PSPF Release 2024 mandates that 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.

See PSPF Guidelines Section 3.1.4—Security Plan Review.

Recommended Approaches

- Security arrangements support the entity's business objectives by identifying and managing risks that could adversely affect achieving those objectives.
- The entity's historical security experience, security performance and past compliance with the PSPF is considered when setting security goals and objectives.
- The entity's areas of exposure, vulnerability or 'target attractiveness' (the value of an entity or its components to an adversary when viewed as a target) is considered when setting security goals and objectives.

3.1.4 Security Plan Review

PSPF Requirement 0020 mandates security plans (and supporting security plans) are considered annually and reviewed at least every two years. A security plan is a 'living' document and requires review and adjustment to ensure the goals and management of security risks keeps pace with changes in the entity and with emerging threats. This could include, for example, a change in the National Terrorism Threat Level or an emerging threat that alters the entity's business impact level, see PSPF Release 2024 (Table 1). It is recommended the security plan also be reviewed when there are significant shifts in the entity's risk or operating environment.

Entities determine how the review of the security plan (and supporting security plans) is conducted. Security plans may be reviewed by the CSO or appointed security practitioner, an external security

consultant or through a security governance oversight committee for larger or more complex business operations.

- Consider – entities are obligated to consider the adequacy of their security plan and supporting security plans each year and decide whether the arrangements are appropriate or a full review is warranted.
- Review – entities are obligated to undertake a review of their security plan at least every two to ensure the plans arrangements are sufficient and clearly articulate how the entity's security risks are managed and how security aligns with other priorities and objectives; and reflects the entity's protective security requirements and mitigation strategies appropriate to the levels of threat, risks to its assets and risk tolerances. The review should also capture decisions for any resulting changes.

Recommended Approaches

- Entities review their security plan when there are significant shifts in the entity's risk or operating environment.

3.2 Security Practices and Procedures

PSPF Requirement 0021 mandates that entities must develop procedures are developed, implemented and maintained to ensure all elements of the entity's security plan are achieved.

Protective security practices and procedures reflect the entity's implementation of PSPF requirements across the six domains and cover all elements of protective security.

This obligation includes establishing any additional entity-specific security policies or procedures that are required above and beyond the PSPF Requirements. For example site-specific procedures, bespoke security situations that are not covered under the PSPF, or where the PSPF specifies 'in accordance with/subject to entity procedures'.

For example, the Department of Defence's Defence Security Principles Framework (DSPF) establishes additional practices and procedures to manage security within their operational context and constraints.

Protective security practices are more likely to be effective in achieving the required protection when they are demonstrated by senior management, embedded into day-to-day operations, and are well understood by all personnel with clear links to why they're important and what they're designed to accomplish.

Recommended Approaches

- Entities develop security procedures in conjunction with other security and risk planning and update these procedures when significant changes in the risk environment occur.
- Establish any entity-specific practices or procedures that are required for the entity's unique operating environment or operational needs.
- Entities put in place measures to monitor the effectiveness of procedures and security performance and update annual security awareness training with relevant messaging.

3.3 Continuous Monitoring and Improvement

PSPF Release 2024 mandates that the entity's security plan must detail the entity's monitoring arrangements and plans to uplift protective security improvement in areas of insufficient implementation. It further mandates that the security plan must include how the entity will review the security plan including 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. See PSPF Guidelines Section 3.1.3 for further guidance on Developing a Security Plan.

Achieving and maintaining compliance with the PSPF and its 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 benefits of effective security maturity monitoring arrangements include:

- understanding of the entity's security risks and risk mitigation strategies
- performance of the entity in:
    - implementing PSPF requirements in relation to its risk environment
    - driving a strong security culture through awareness of agreed security behaviours
    - identifying and implementing changes that achieve robust security outcomes, and
    - using resources efficiently and effectively to protect people, information and resources
- assurance that the entity's:
    - people, information and resources are adequately protected consistent with government policy, and
    - security risks are managed appropriately (including security incidents) and clear lines of accountability and sound planning and proportionate reporting are undertaken.

Recommended Approaches

- Develop their security maturity monitoring plan as part of their overarching security plan. This includes:
    - using security maturity indicators as detailed in the PSPF Risk-Based Compliance Reporting Model
    - setting goals and objectives and identifying the impact on security of any goals and objectives detailed in the entity security plan
    - developing methodologies to manage the collection, measurement and analysis of data in relation to the entity's security maturity indicators
    - determining the frequency of security monitoring advice to be given to the Accountable Authority, CSO, audit committee and relevant security governance committee (if established in the entity)
    - setting pre-determined levels of change in security maturity metrics that trigger escalation to the Accountable Authority, CSO, audit committee and relevant security governance committees, and
    - where applicable, identifying the responsible area and timeframes to:
        - manage implementation of PSPF requirements
        - implement strategies that achieve improvements in security culture.

3.3.1 Monitoring cycle

Table 10: Monitoring Cycle Components

Component	Details
Plan	The entity security plan is prepared and approved.
Collect	Collect evidentiary documentation, information and data, including: • performance of compliance with PSPF requirements and standards • security incident and near miss reporting • security investigation reports and learnings • systematic and routine audits of entity security practices and procedures • security awareness training results and feedback • direct observations and security facility inspections • feedback from the security governance committee or other key security stakeholders • reviews of entity security practices and commissioned research • internal focus groups and security questionnaires • stakeholder consultation • horizon scanning for early identification of emerging security issues internal and external to government that may impact security maturity.
Assess	Assess the security plan's evidentiary documentation, information, data and corresponding performance measures to identify areas of low or insufficient implementation of protective security requirements or poor practice. Determine amended mitigation strategies to address the issues identified.
Remediate	Make necessary adjustments to practices, performance, culture or capability and implement amended mitigation strategies.
Review	Review the strategies and implementation pathways identified in the security plan to ensure expected results are being achieved within an appropriate and predetermined timeframe, and that unmitigated risks are addressed. Pinpoint areas for improvement.
Improve	Implement agreed strategies to address areas of improvement. Use monitoring arrangements throughout the year to inform improvements and use learning from any security incidents to inform the next security plan review.

3.4 Positive Security Culture

PSPF Release 2024 mandates that the Accountable Authority and CSO are responsible for developing, implementing and maintaining a program to foster a positive security culture in the entity with clearly defined security expectations and priorities. They are supported by the entity's CISO and security practitioners to promote a culture where personnel value, use and protect entity information and resources appropriately.

A positive security culture is vital to effectively and securely delivering Australian Government business. This is reflected in PSPF Principles:

1: Security is everyone's responsibility.

2: A positive, embedded secure culture is critical.

3.4.1 Security Culture Definition

Culture is a difficult idea to define precisely. Broadly, a culture consists of the values, behaviours and other characteristics common to the members of a particular group. Security culture is best understood as an amalgam of a diverse range of security experiences, which occur as a result of an intersection of people (both security personnel and other entity staff), policy, business need and circumstances. Security culture is expressed through patterns of accepted security behaviours, and the beliefs and values that promote and reinforce them.

This experience is highly variable across (and within) entities, leading to a range of security cultures not only within an entity but across government. The Australian Government comprises a diverse range of entities. This means there are differing cultures, risks and attitudes towards security in each entity. Even within a single entity, while personnel may share an identity (for example, 'professional' or 'service-oriented'), there is often not one culture, but many. Embedding positive security attitudes and behaviours within this diversity is challenging, but essential to achieving protective security outcomes.

3.4.2 Positive Security Culture

An entity with a positive security culture encourages and enables personnel to engage with security in an appropriate manner and makes informed decisions on security and the risks, within agreed entity security risk tolerances

A positive security culture is fostered through the shared values, approaches and behaviours that an entity and its personnel adopt towards security, to address security threats and risks. It can be moulded by proactive actions and activities that encourage change in the patterns of accepted security behaviours of staff and management.

A positive and effective security culture is one where:

- security is prioritised and promoted across the entity by the Accountable Authority, CSO, CISO and senior leaders
- security is built into an entity's business operations
- security is an enabler of business, supporting accessibility of services
- security risks are identified and managed and personnel understand those risks and their responsibilities in relation to them
- security awareness training is effective in ensuring all personnel, including contractors, understand their obligations and responsibilities, including:
    - aware that security is everyone's responsibility
    - able to understand and comply with security-related obligations and entity-specific practices and procedures
    - equipped and supported to engage with risk and make risk-based decisions
    - aware of the consequences of non-compliance with security practices and procedures
    - comfortable to challenge others on non-compliance with entity security practices and procedures
    - confident in making decisions on applying protective markings, storing and sharing government information

- security incidents and breaches are reported, recorded and investigated appropriately according to clear entity procedures
- implementation of protective security policies is mature and well-managed
- entity security procedures are easy to understand, current and visible to all personnel
- classified information is protected from unauthorised disclosure or compromise and personnel apply the need-to-know principles, and
- security improvements are encouraged and promoted within the entity.

Developing an active and robust security culture can significantly decrease the threat to an entity and its operations. In turn this will improve security culture across government and underpin the continuous and safe delivery of government business and the protection of its resources. In addition to help keep entities and their personnel safe from threats, a healthy and positive security culture helps to increase internal and external trust, create consistent positive behaviour, and engage productively with risk.

The path to achieving a positive security culture that is resilient to change is not a straight line and will look different for each entity.

3.4.3 Factors that Transform Security Culture

The following factors are critical to transform the entity's security culture.

3.4.3.1. Build Capability of Senior Leaders to be Security Champions

When senior leaders champion security, it shows they understand the importance of successfully embedding security into the entity's culture and have the knowledge and skills to lead by example, modelling good security practices and behaviour.

When security is prioritised and supported by senior leaders, the appetite to understand, prioritise and apply protective security appropriately filters down throughout the entity.

Measures of success include:

- Accountable Authority, CSO and CISO are engaged in security matters and leading by example
- security will no longer be seen as 'not my job' but a key component of everyone's responsibilities, and
- cross-entity engagement to resolve emerging security issues.

3.4.3.2. Ingrain Security Behaviours at All Levels

A strong security culture is built on a foundation of effective security awareness. Improving the quality of security awareness by providing training (and the annual refresher training) and supporting materials that are practical, clear and easily understood will help build the security capability of personnel.

Security awareness training also ensures personnel understand their security obligations and how to apply their entity's security procedures and practices.

Psychological barriers to positive security behaviours are reduced and new habits are formed, with security becoming part a natural and instinctive part of daily work of an entity's personnel.

To make sure this security capability is applied (rather than seen as an additional burdensome obligations) behavioural economics approaches may be effective to building the 'security muscle memory' of all

personnel, ensuring that security is ingrained in everyday behaviour. Approaches that reward good behaviour and encourage good practice is an effective way of protecting against poor security practices.

Measures of success include:

- protective security culture and capability improves
- security is ingrained into everyday behaviours, personnel build 'security muscle memory' and find security obligations less burdensome
- security incidents are appropriately reported by personnel and learnings of these incidents are used to inform amendments to security awareness training programs, and
- the severity and frequency of repeated security incidents are reduced and learnings of these incidents are used to inform amendments to security awareness training programs.

3.4.3.3. Equip Personnel to Effectively Engage with Security Risk

To effectively engage and manage security risks requires:

- clear understanding of the entity's risk tolerances and appetite for types of security risk
- clearly defined responsibilities for security risk management, and
- support from senior leaders to manage risks, make risk decisions within appropriate areas of control, and learn from mistakes.

Measures of success include:

- security risks, including any residual risks, are well managed and effective in ensuring the protection of people, information and resources
- personnel at all levels exhibit confidence to manage security risks within the ranges of the entity's risks tolerances
- security risk management is demystified and forms part of the entity's enterprise risk management process, and
- security processes identify changes in the threat environment and allow for adjustments to maintain acceptable levels of risk, balancing operational and security needs.

3.4.3.4. Integrate Security into the Design, Development and Delivery of Government Business

Embedding security into the development of business processes and decision-making will help ensure practical outcomes for both security and business problems. If security is not seen as an optional 'add-on' or retrospectively fitted but rather a key component of delivering government business, we will shift perceptions about functionality so that functional includes secure. This will also address concerns that improving security behaviours and practice is too burdensome, as well-designed security provisions should not impede functionality.

Measures of success include:

- security is integrated as a key component of the entity's business planning and development, implementing security-by-design principles, and
- security risk management decisions shift from reactive decisions (post-incident) to pre-emptive decisions to employ appropriate mitigations and resources.

See ASD's Secure-by-Design Foundations

3.4.3.5. Normalise Information Sharing to Understand and Address Security Risk

Entities are encouraged to share protective-security related information, learnings and training materials with other government entities, particularly those in the same portfolio. Sharing lessons learnt reduces the need for entities to invest money and resources on recreating processes and systems (for example training materials and mitigations).

Entities can share materials on the Protective Security Policy GovTEAMS community.

Measures of success include:

- entities that lack capability or resources are supported
- improved consistency of application across government, and
- more efficient and cost effective use of government resources.

3.4.4 Factors that Undermine Security Culture

A lack of implementation of security policy and awareness—of both Government's expectations for good security practice and the security environment in which personnel are working—has the potential to breed complacency towards positive security behaviours, introducing a range of vulnerabilities to the secure delivery of government business and exposing the government to significant risk.

The key factors that undermine a positive security culture in government are:

- misalignment between security and senior leaders
- lack of confidence by personnel to engage with security risk
- security viewed as a barrier to entity operations or business
- fear as the only motivator to comply
- security designing for itself, and
- ineffective security training and security procedures.

3.5 Security Awareness Training

A robust and positive security culture 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.

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 supports the consistent application of protective security practices and procedures across the entity. However, policies and procedures will not be effective if people do not understand them or why they are needed, or are not aware of them, or are unable to follow them.

Furthermore, although the majority of entities have security awareness training and education tools, the experience of security training and guidance is highly variable. Attitudes to security range from the highly motivated and aware, to the disengaged and unaware, as well as the conscious opponents who deliberately choose not to comply.

PSPF Requirement 0024 mandates that all personnel (including contractors) receive security awareness training at engagement and annually thereafter. This obligations includes providing personnel with sufficient information and training on their protective security responsibilities.

3.5.1 Effective Security Awareness Training

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, and
- clearly communicates to all personnel, including contractors, the entity's protective security practices and procedures.

Recommended Approaches

- CSO considers the entity's risk and current threat environment, goals and objectives of the entity's security plan, and any identified inadequacies in previous methods of training or consistent failure to understand content, particularly when systemic or repeated security incidents indicate potential vulnerabilities in awareness training.
- CSO decides the most appropriate delivery method for security awareness training to ensure consistent delivery within their entity and others the entity provides training to as part of a lead security arrangement.
- Security awareness training is tailored to your entity's risks, security practices and procedures and functions.
- Security awareness training is practical and promotes personal responsibility for protective security, regardless of the role or level of seniority in the entity.
- Security awareness training uses a mixture of delivery methods and follows principles of adult education.
- If used, outsourced training providers of security awareness training have sufficient knowledge of the PSPF and expertise in delivering adult education.

3.5.2 Security Training Activities

All entity personnel need to understand their protective security responsibilities and be aware of how Australian Government security classified information and resources are vulnerable to compromise or misuse. Establishing training activities is an effective way to promote awareness, reinforce the practical actions that each person can take to contribute to the entity's security posture, and support the entity's efforts to manage the insider threat.

Entities are encouraged to strengthen security awareness through:

- campaigns that address the ongoing needs of the entity and the specific needs of Security Zones or classified activities

- education and promotion materials including instruction guides, checklists, cheat sheets, reminders via publications, electronic bulletins and visual displays such as posters
- security zones are clearly defined so personnel know what information and devices can be used, stored and carried in each zone
- protective security-related questions in personnel selection interviews
- drills and exercises
- dedicated Security Awareness Week, and
- inclusion of security awareness and attitudes in the entity performance management program.

3.5.3 Delivery of Security Awareness Training

There is no fixed delivery method for security awareness training. When delivering training, entities are also recommended to include:

- advice to personnel on entity-specific asset management and loss reporting procedures prior to them taking custody of assets, including entity fraud measures
- a safety handbook for all personnel that includes emergency response guidelines and contacts, as well as entity-specific safety requirements and procedures
- personnel with specific emergency safety or security roles with regular training, as well as assessment of their ongoing competency
- specialist training to meet entity-specific risks, and
- targeted security awareness training where the entity has identified a need based on their risk profile, or when the entity has an increased or changed threat environment.

3.5.4 Content of Security Awareness Training

Security awareness training programs or briefings for all personnel are recommended to include:

- Personal safety and protective security responsibilities
    - security measures in entity facilities and in the field
    - individual and line manager security responsibilities
    - overseas travel safety and security
    - identifying unusual and suspicious behaviour (insider threat)
    - employment suitability ongoing obligations, including any entity-specific reporting requirements
- Entity protective security arrangements, procedures and security culture
    - understanding entity-specific security risks and threats
    - policies and procedures that are in place to mitigate or manage these risks and threats
- Protecting and handling official information and resources
    - confidentiality, integrity and availability requirements for information and resources, including intellectual property
    - assessing the value, importance and sensitivity of information and applying security classifications, security caveats, and where used, information management markers

- protections for security classified information, including handling of security caveated information
- applying the need-to-know principle
- understanding how to share information in the entity, across government and with external stakeholders

- Reporting obligations
  - reporting security incidents (including compromise of information, breach of entity procedures, data spills etc.)
  - contact reporting, including the Contact Reporting Scheme
  - reporting concerns about other personnel, including their suitability to access Australian Government resources
  - any other entity-specific reporting requirements including public interest disclosure (whistleblowing) under the *Public Interest Disclosure Act 2013*.

Previously reported or investigated security incidents can be used in security awareness training as examples that demonstrate what could happen, how to respond to incidents, and how to minimise them in the future. If used, redact security classified information to maintain appropriate confidentiality.

3.5.5 Additional Content for Security-Cleared Personnel

As a minimum, security awareness training programs or briefings for security-cleared personnel should:

- ensure that all personnel accessing security classified information or resources, understand and accept their day-to-day security responsibilities and reporting obligations (e.g. changes of circumstances, and suspicious, ongoing, unusual or persistent contacts)
- provide clearance holders with regular updates, briefing and training to remind them of their clearance responsibilities
- include training and briefings for personnel with access to security caveat information and Sensitive Compartmented Information, in consultation with compartment owners.

3.5.6 Additional Content for High-Risk Positions

PSPF Requirement 0025 mandates that entities must provide personnel in specialist and high-risk positions (including contractors and security incident investigators) with specific security awareness training to address the risks related to the nature and scope of their work or specialisations.

Specialist or high-risk positions could include:

- sensitive or priority negotiations or policy work
- responsibility for or access to valuable or attractive resources
- working remotely or in dangerous conditions, or
- being required to liaise with foreign officials, or regularly share information with foreign officials.

3.5.7 Security Awareness Refresher Training

PSPF Requirement 0024 mandates that entities provide personnel with security awareness training at engagement and annually thereafter. The CSO determines the form (e.g. in person, virtual, self-paced), scope of coverage and content required for the annual training requirement to maintain sufficient

awareness of security requirements and obligations to protect the entity's people, information and resources.

Security awareness training is not a once and done exercise, it requires regular reinforcement and updating to ensure it remains effective. Annual refresher training is designed to remind personnel about their protective security obligations and advise them of any recent changes in the entity's risk or operating environment and any new security arrangements.

When updating the entity's annual security awareness training materials, consider whether amendments need to be made to:

- accommodate changes in the entity's risk and current threat environment
- acknowledge key shifts in the entity's goals and objectives (as listed in the security plan) or security arrangements and procedures, or
- address inadequacies identified in previous methods of training or consistent failure to understand content, particularly when systemic or recurring security incidents indicate potential vulnerabilities in awareness training.

Recommended Approaches

- Security drills and exercises are regularly carried out to gauge people's knowledge and the effectiveness of the entity's security awareness training.
- Security awareness training is updated annually to reflect the annual PSPF release, any changes in the entity's operations or security arrangements, and to address inadequacies in previous training methods.

3.6 Security Incidents

Managing security incidents helps monitor security performance, identify inadequacies in security procedure, and detect security risks in order to implement appropriate treatments. Through effective reporting and investigation of security incidents, entities can identify vulnerabilities and reduce the risk of future occurrence.

A security incident might have wide-ranging and critical consequences for the entity and the Australian Government. In recognition of the potential consequences, managing security incidents is an important function of the CSO, and of the CISO for cyber security incidents.

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, resources or activities
- approach from anybody seeking unauthorised access to official resources, or
- event that harms, or may harm the security of Australian Government people, information, resources or activities.

Examples of Security Incidents

- Criminal actions such as actual or attempted theft, break and enter, vandalism or assault.

- Loss of personal information that is likely to result in serious harm. In some circumstances, the loss of personal information may be considered a security breach – refer to OAIC's Notifiable Data Breaches scheme.
- Security classified material not properly secured or stored.
- Security classified material left in inappropriate waste bins or government assets to be disposed of or sold.
- Deliberate disregard of implementing a PSPF requirement.
- Access passes or identification documents lost or left unsecured.
- Incorrect handling of security classified information, such as failure to provide the required protection during transfer or transmission resulting in a data spill on an electronic information network or system.
- Compromise of keys to security locks, or of combination settings.
- Sharing computer passwords.
- Vandalism.
- Inadvertent loss of entity or personal data through limited cyber literacy, for example lack of awareness that graphs or tables copied from Microsoft Excel to Microsoft Word may include embedded information that requires security protection, and that saving as a PDF may not necessarily lock down that data.

Where a suspected security incident involves the major compromise of official 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.

3.6.1 Significant Security Incidents

A significant security incident is generally one that is considered to be serious or complex. The CSO is responsible for establishing monitoring mechanisms across the entity, and for managing the entity's response to security-related crises, incidents and emergencies (other than those related to cyber security) in accordance with the entity's security incident and investigation procedures. This includes determining when a security incident is considered significant and therefore reportable. In the same way, the CISO is responsible for cyber incidents.

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 triggers external incident reporting or referral obligations.
- 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, resources or activities, 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.

Examples of Significant Security Incidents

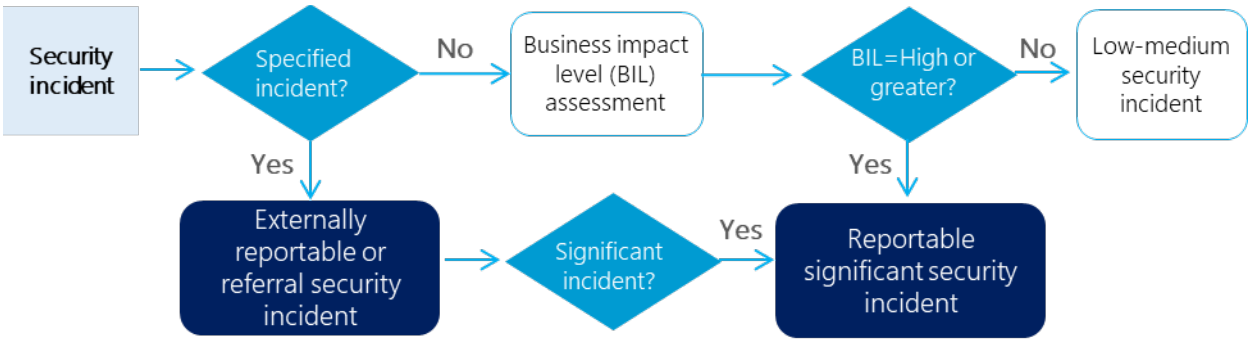
- Espionage or suspected espionage.
- Actual or suspected compromise of material at any level, including tampering with security containers or systems.
- Loss, compromise, suspected compromise, theft or attempted theft of classified equipment.
- Actual or attempted unauthorised access to an alarm system covering a secured area where security classified information is stored.
- Loss of material classified PROTECTED or above, or significant quantities of material of a lower classification.
- Recovery of previously unreported missing classified material or equipment.

- Unauthorised disclosure of official or security classified information, significant loss or compromise of cryptographic keying material, or a significant breach of technology systems as assessed ASD.
- Continuous breaches involving the same person or work area where the combination of the incidents warrants an investigation.
- Loss, theft, attempted theft, recovery or suspicious incidents involving weapons, ammunitions, explosives or hazardous materials including nuclear, chemical, radiological or biological.
- Actual or suspected unauthorised access to a technology system.

Table 11: Recommended Delegations for Security Incidents

Business Impact Level	Potential (or Actual) Harm to the National Interest, Organisations or Individuals	Delegation	Externally Reportable
1 Low business impact	Insignificant Damage	As per entity's procedures	No
2 Low to medium business impact	Limited Damage	CSO, CISO (for cyber incidents), or delegate	CSO, CISO (for cyber incidents), or delegate to decide
3 High business impact	Damage	CSO or CISO (for cyber incidents)	Yes
4 Extreme business impact	Serious Damage	CSO or CISO (for cyber incidents)	Yes
5 Catastrophic business impact	Exceptionally Grave Damage	CSO (and CISO for cyber incidents) in consultation with Accountable Authority	Yes

Figure 2: Decision-making process to determine reportable security incidents



Example

Entity Y detects a cyber security incident of a type that triggers reporting to ASD. Following PSPF Requirement 0028 and PSPF Release 2024 (Table 2) and ISM control 0140, Entity Y immediately reports the incident to ASD and seeks their assistance with remediation. The technology system that is impacted by the incident also provides services to Entity Z, so, applying PSPF Requirement 0028 Entity Y contacts Entity Z's CISO to advise them of the incident and the remediation work underway.

Entity Y's CISO then determines that the potential BIL of the incident is high business impact. Following PSPF Requirement 0028, Entity Y reports the incident to Home Affairs via the PSPF Reporting Portal. Once the incident is remediated, Entity Y shares the lessons learned during the incident in their annual protective security report.

See PSPF Release 2024 (Table 2) for information on where to report for externally reportable incidents.

See Table 18 for the Business Impact Level Tool.

Other factors the CSO (or CISO) should consider in determining whether an incident is significant and therefore reportable are:

- widespread impact or if there are multiple entities involved, for example through shared service arrangements, where the target provides services to other entities
- value, importance or sensitivity of the information, data or systems involved in the incident, for example compromise of large data sets or aggregated information make raise the significance of the incident
- extent of the compromise, for example was it a 'one-off' isolated incident or likely to be extensive or sustained with ongoing or worsening effects, and
- secondary impact, for example, if the incident escalates over time.

3.6.2 Coordination of Cyber Security Incidents

ASD'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. ASD defines a cyber security incident as an unwanted or unexpected cyber security event, or a series of such events, that has either compromised business operations or has a significant probability of compromising business operations.

The National Cyber Security Coordinator coordinates responses to major cyber security incidents, whole-of-government incident preparedness efforts, and strengthens Australian Government cyber security 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, in collaboration with the National Cyber Security Coordinator and the National Emergency Management Agency, to ensure that consequence management is activated as appropriate.

3.6.2.1. Security Exercises

A security exercise is an activity that assesses, tests and validates the entity's ability and preparedness to detect, respond to and recover from security incidents. It can be a single activity or a series of activities that allow participants to practice responding to an event or incident, delivered in a safe environment to allow learning and improvement.

A security exercise tests whether the entity's security incident management plans and procedures are appropriate and effective, and its personnel are ready and capable of responding to security incidents. The exercise may be run by a single entity or in collaboration with one or more entities, industry partners or external stakeholders.

Security exercises and preparedness activities can take many different forms, including:

- Discussion-based exercises, such as table-top exercises or scenario-based exercises to work through hypothetical but realistic security incidents.
- Procedural drills and exercises to test the validity of entity procedures and decision-making arrangements.
- Intelligence-based exercises.
- Scenario exercises, providing a realistic notion of an event or security incident.

- Threat hunting or penetration testing exercises.
- Simulation exercises, including pervasive compromise simulations, unlawful interference activities, or red team (offensive/attackers) vs blue team (defensive/defenders) exercises.
- Hybrid exercises, covering multiple types of exercises either concurrently or consecutively.

Useful resources:

  - ASD's Exercise in a Box – provides cyber security exercises that entities can use to assess and improve their cyber security practices and preparedness
  - CISA's Tabletop Exercise Packages and After Action Report Template

3.6.3 Security Incident Management and Exercises

PSPF Requirement 0026 mandates that procedures are developed, implemented and maintained to ensure security incidents are managed and responded to.

Many potential security incidents are observed by personnel. It is important that all personnel, including contractors, understand how and when to report potential incidents or concerns. Security awareness training should cover this content.

Procedures for managing security incidents should include:

- personnel, including contractors, immediately reporting security incidents to a centralised point in the entity (CSO, CISO or security practitioners) and include arrangements for personnel travelling or working remotely
- formal procedures and mechanisms to make it easy to report security incidents (including responding to and investigating incidents that occur outside of the entity's premises)
- handling procedures once a security incident has been reported, including:
  - clearly defined roles and responsibilities (of personnel involved in the administration of security incidents and the conduct of investigations)
  - escalation points, relationships and connection points (internal or external) and communication channels
  - timeframes for incident response and recovery
  - assessment and categorisation of the level of harm or compromise
  - technical requirements and continuity
  - prioritisation where multiple incidents or events occur simultaneously
  - addressing entity-specific issues or incident types
  - linkages to other entity procedures such as business continuity or disaster recovery plans
  - reporting to the CSO, CISO (for cyber incidents) and security governance committee, and
  - testing and review cycles
- security practitioners maintaining records of reported incidents and any other security incidents, and
- suitable feedback processes to ensure that personnel reporting information security events are notified of results after the issue has been dealt with and closed.

The steps for managing security incidents are:

- Detect security incidents
- Report and remediate security incidents
- Record security incidents, and
- Learn from security incidents.

Recommended Approaches

- Where security investigation functions are shared across entity work areas or with an outsourced service provider, the CSO, CISO (or another delegated SES officer) should maintain oversight of the investigation and establish mechanisms to monitor the investigation and ensure communication of issues, findings and decisions to all relevant parties.
- Simple channel for personnel (including contractors and personnel travelling or working remotely) to report security incidents, or suspected incidents, is established to promote timely reporting.
- Security awareness training covers reporting security incidents and provides practical examples and potential consequences.

3.6.3.1. Detect Security Incidents

It is critical that security incidents are detected early and reported to the CSO, CISO or security practitioner in order to expedite protection, containment and recovery in response to the incident.

The availability of appropriate data sources is key to detecting security incidents. While personnel reporting security incidents is a common means of detection, the CSO and CISO should consider other identification and monitoring methods to supplement reporting of incidents.

The CSO, CISO or security practitioner is recommended to assess the security incident and identify if further action or an investigation is required, including to:

- confirm it is a genuine security incident rather than a false alarm or vexatious complaint
- determine the type of incident and scale of harm resulting from the incident
- decide what action is required to address the incident (by whom and when), for example:
  - no further action
  - amendments to entity procedures, systems or training
  - containment, recovery or eradication action required
  - training or performance management activities with the individual/s involved in the incident
  - security investigation
  - escalation to CSO, Accountable Authority or responsible Minister, or
  - external reporting or referral to appropriate authority (see PSPF Requirement 0028 and PSPF Release 2024 Table 2).

See ASD's Guidelines for Cyber Security Incidents | Cyber.gov.au for further guidance on detecting cyber security incidents.

3.6.3.2. Report and Remediate Security Incidents

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 also develops, implements and maintains procedures to ensure security incidents are responded to and, where required, appropriately investigates, and exercises these arrangements.

Security procedures for reporting security incidents should:

- require personnel, including contractors, to report security incidents to a centralised point in the entity (for example to CSO or security practitioner)
- specify the roles and responsibilities of personnel involved in the administration of security incidents and the conduct of investigations
- establish formal procedures and mechanisms to make it easy to report security incidents
- require the security practitioners to maintain records of any reported incidents and any other security incidents, and
- have suitable feedback processes to ensure that personnel reporting information security events are notified of results after the issue has been dealt with and closed.

PSPF Requirement 0028 mandates that significant or externally reportable security incidents and referral obligations are reported to the relevant authority (or authorities) within the applicable timeframe. See PSPF Release 2024 (Table 2).

Some security incidents have more than one line of reporting and may require the entity to report to multiple relevant authorities. In such cases, the following reporting order is recommended:

- Report internally – apply entity security incident reporting procedures to inform the entity's CSO (or their delegate for incidents below low to medium business impact) or CISO for cyber incidents, and obtain a decision on whether the incident triggers external reporting obligations.
- Report to the relevant authority – apply PSPF Release 2024 (Table 2) to seek assistance with containment, remediation and meet reporting and referral obligations within the timeframe specified by the relevant authority.
- Report to other affected entities – inform the CSO, CISO or Accountable Authority of the entity whose people, information or resources are, or may be, affected by the incident (see Australian Government Directory), and any other parties with a need-to-know about the incident, regardless of whether the incident is deemed significant or not.
- Report to the Department of Home Affairs – apply PSPF Requirement 0028 to alert the PSPF policy owner that a significant security incident has occurred and to share any 'lessons learned' in response to the incident, including where the incident points to areas for improvement in the PSPF policy or guidance. Lessons from the incident are often not identified at the time the incident occurs, or until after an investigation is complete. To supplement this reporting obligation, entities are also required to provide details in the entity's annual protective security report of any lessons learned from significant security incidents that occurred during the reporting period.

Recommended Approaches

- ✔ Additional identification and monitoring detection methods are established to supplement reporting of security incidents by personnel.
- ✔ Establish internal reporting and recovery plans.

Reporting Significant and Reportable Security Incidents

A significant security incident is a deliberate, negligent or reckless action that leads, or could lead to, the loss, damage, compromise, corruption or disclosure of official resources. A significant security incident can have wide ranging and critical consequences for the entity and the Australian Government.

PSPF Requirement 0028 mandates that entities report significant and reportable security incidents at the time they occur to:

- the relevant authority, as detailed in PSPF Release 2024 (Table 2)
- other affected entities, and
- the Department of Home Affairs.

Reporting Security Incidents to the Relevant Authority

To fulfil PSPF Requirement 0028, entities must first report any significant or reportable security incidents to the relevant authority as detailed in PSPF Release 2024 (Table 2).

Entities are required to report to the relevant authority once they become aware that the security incident has occurred or is occurring.
Some authorities set specific timeframes for reporting, see PSPF Release 2024 (Table 2).

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. It further ensures the relevant authority is aware of the types and numbers of security incidents occurring with their area of responsibility.

Details of significant and reportable security incidents and the relevant authority to which entities report are provided in this table and summarised below:

- Significant national security-related incidents—ASIO
- Significant cyber security incidents—ASD
- Security incidents involving Cabinet material—PM&C
- Security incidents involving personnel with a security clearance—Australian Government Security Authorised Vetting Agency (or entity CSO if the entity is an Authorised Vetting Agency)
- Contact reporting—ASIO Australian Government Contact Reporting Scheme
- Correspondence of security concern—ASIO
- Security incidents or unmitigated security risk that affects the protection of another entity's people, information or assets—Accountable Authority (or CSO) of the affected entity
- Security incidents involving security classified equipment and services—Security Construction and Equipment Committee
- Security incidents involving a foreign entity's assets or information—entity CSO. The incident may also need to be externally reported in line with other reportable incident categories.
- In addition, some security incidents may be subject to other legislative or policy reporting requirements, for example:
    - eligible data breaches must be reported to the OAIC under the Notifiable Data Breaches Scheme

- potential criminal/serious incidents must be reported to the AFP (crimes against the Commonwealth of Australia) or local police (state and territory crimes), or
- critical incidents involving public safety must be reported to the Australian Government Crisis Coordination Centre.

Note: There may be other legislative requirements for reporting security incidents.

To avoid inadvertently compromising an open security investigation entities are encouraged to contact the relevant authority or affected entity as early as possible about the incident.

Reporting Significant Incidents to Other Affected Entities

PSPF Requirement 0028 also requires entities to report any significant security incidents or unmitigated security risks that affect another entity's people, information or assets, particularly where entities are co-located or are providing services to another entity.

Reporting Significant Security Incidents to the Department of Home Affairs

PSPF Requirement 0028 also requires entities to report any significant security incidents to the Department of Home Affairs at the time they occur.

The purpose of this obligation is to alert the PSPF policy owner that a significant security incident has occurred and, to share any 'lessons learned' in response to the incident, including where the incident points to areas for improvement in the PSPF policy or guidance.

To fulfil the obligation to share 'lessons learned' from any incidents, investigations, reports or reviews relating to the incident, entities are required to include details of any lessons learned in the:

- significant security incident report at the time the incident occurs, and
- entity's annual security report.

This additional reporting acknowledges that 'lessons learned' may not be identified until after the incident is contained, or after any investigation, report or review is completed.

The obligation to report to the Department of Home Affairs is in addition to the reporting requirements outlined in PSPF Requirement 0028, which state:

- A significant cyber security incident is reportable to both ASD and the Department of Home Affairs
- A significant national security incident is reportable to both ASIO and the Department of Home Affairs.

Information gathered on significant security incidents assists the Department of Home Affairs to:

- determine the adequacy of protective security policies
- provide an insight into entity security culture
- share lessons from the incident and any subsequent investigation, reports or reviews, including where appropriate, across government, and
- identify potential vulnerabilities in government security awareness training to inform whole-of-government security outreach activities.

To lodge a significant security incident report with the Department of Home Affairs:

- PSPF Reporting Portal – for significant security incident reports up to and including PROTECTED

- Secure means appropriate for the security classification – for significant security incident reports at SECRET or above.

Table 12: Reporting Significant Security Incidents to Home Affairs

Classification of Security Incident	Channel for Reporting	Contact
Up to and including PROTECTED	Submit security incident report via the PSPF Reporting Portal.	Email: PSPF@homeaffairs.gov.au to gain access to the PSPF Reporting Portal
SECRET or TOP SECRET	Submit PSPF Offline security incident reporting template via commensurate classified system	Contact PSPF Hotline (02) 5127 9999 for advice

3.6.3.3. Record Security Incidents

Maintaining a record of security incidents provides the CSO and CISO (for cyber incidents) with a valuable source of data to obtain insight into an entity's security environment and performance, while regular analysis of the data enables the CSO and CISO to identify systemic issues and trends. For example, multiple minor security incidents could indicate poor security awareness and could alert the entity to the need for increased security training and education.

It is appropriate that procedures for responding to serious security incidents are formal. This reflects the significance these deliberate or reckless actions may have on security.

After an incident has been contained, it may be necessary for eradication or recovery action to be taken to restore information or systems. See Guidelines for Cyber Incidents for guidance on managing cyber incidents.

Entities can develop mechanisms for recording incidents that best suit their security environment and operational requirements.

Recommended Approaches

- Record the details of each reported security incident, including:
  - time, date and location of security incident, including how the incident was detected
  - type of official resources involved
  - description of the circumstances of the incident, including any personnel or locations involved
  - nature or intent of the incident, e.g. deliberate or accidental
  - assessment of the degree of compromise or harm
  - whether it is an isolated incident or part of a broader reoccurring issue, and a
  - summary of immediate action (including containment or eradication) and any long-term action taken (including post-incident activities).
- CSO and CISO (for cyber incidents) maintains oversight of recorded security incidents and regularly analyses them to identify trends and systemic issues.
- Complete a post incident review of significant security incidents to identify areas for improvement and where required, update training, security incident management plans and security exercises,

3.6.3.4. Learn from Security Incidents

Lessons from the incident are often not identified at the time the incident occurs, or until after an investigation is complete. To supplement the obligation to report significant security incidents to the Department of Home Affairs, entities are also required to provide details of any lessons learned from significant security incidents that occurred during the reporting period, in the entity's annual protective security report.

Embedding post-incident learning into incident reports or updated procedures can provide useful insights into opportunities for improvements and emerging issues, vulnerabilities in processes and training, or personnel's understanding of how to apply security obligations. This supports a process of continual improvement for monitoring, evaluating, responding to and managing security incidents.

Possible questions to consider once the incident is resolved:

- Were the procedures adequate to deal with the incident and were all stages of incident management followed?
- Were the right people involved and were escalation points and timeframes sufficient and useful?
- Did the incident highlight areas of vulnerability and if so, what action is being taken to address these vulnerabilities?
- Could the incident have been prevented? If so, how?
- Could the incident have been detected earlier, or damage reduced if detected earlier?
- What were the triggers and is there a way to prevent future occurrences?
- Is it a repeated incident or is the type of incident becoming systemic, if so, what additional protection or action is required to prevent further incidents?

Recommended Approaches

- ✔ Identify, document and share learnings internally (i.e. with and between the Accountable Authority, security practitioners and security governance committee) and externally, where appropriate (i.e. with co-located entities, entities with similar risk profiles or through whole-of-government arrangements).
- ✔ A post incident analysis is conducted after each significant security incident to identify areas for improvement and lessons learnt to inform handling of future incidents.
- ✔ Information gathered from security incidents informs is used by CSO/CISO to determine the adequacy of protective security practices, measure security culture, highlight vulnerabilities in security awareness training and inform security improvement activities.

3.6.4 Externally Reportable Security Incidents and Referral Obligations

PSPF Requirement 0028 mandates that entities must report any significant or externally reportable security incidents and referral obligations to the relevant authority (or authorities) within the applicable timeframe.

Each entity may have a different threshold for determining when an incident is significant enough to report. However, PSPF Release 2024 (Table 2) details when external reporting obligations are automatically triggered and details of the delegation for decisions. See Figure 2: Decision-making process to determine reportable security incidents.

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.

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
- gathers evidence that may be admissible for any subsequent action whether under criminal, civil penalty, civil, disciplinary or administrative sanctions
- prevents re-occurrence of the incident by implementing improvements to entity systems or procedures, and
- protects both the interests of the Australian Government and the rights of affected individuals.

PSPF Requirement 0029 mandates that procedures are developed, implemented and maintained to investigate security incidents in accordance with the principles of the Australian Government Investigations Standards (AGIS).

The AGIS were developed to ensure quality investigative practices and outcomes in entities. The principles guiding and reinforcing AGIS apply to all security investigations.

Responsibility for investigating security incidents sits with the CSO, with support from the CISO for investigations into cyber security incidents and for establishing procedures that cover:

- terms of reference and the investigation plan, authorised by the CSO, CISO or other SES officer
- responsibilities, including the investigator, approving officer and other relevant parties
- qualifications and training required for investigators
- procedural fairness and standards of ethical behaviour to ensure the investigator is impartial, without actual or apparent conflict of interest in the matter being investigated
- actions on receiving a complaint or allegation, including anonymous allegations or reports from whistle blowers
- case management procedures to ensure any case records, activities, recommendations and decisions adhere to the agreed process (AGIS is the recommended standard)
- procedures for operational practices such as interviewing anyone whose interests could be adversely affected by the outcome of a security investigation, or anyone who may be able to assist with a security investigation
- referral points to ASIO, the relevant law enforcement service and ASD
- decision points and agreed escalation and approval phases, including keeping the CSO, CISO or delegated officer informed of the investigation's progress
- major findings and recommendations, and
- arrangements for the final investigation report.

Not all security incidents warrant investigation[2]. The CSO or CISO (for cyber incidents) determines when a security incident is serious or significant enough to commence an investigation. Investigating security incidents (actual or suspected), may be necessary to resolve an existing breach or vulnerability and remediate the impact. An investigation may provide valuable information for future risk reviews and assessments and will help entities to evaluate current security plans and procedures.

Once the CSO, CISO or appointed security practitioner has established the need for an investigation, they are encouraged to determine:

- the seriousness or complexity of the incident
- the nature of the possible outcome of the investigation (administrative, disciplinary, civil or criminal)
- if the incident is criminal in nature and needs to be referred to an external entity
- the resources needed to conduct the investigation
- who is the best placed or qualified person to complete the investigation and what support they need
- an agreed investigation process including timeframes
- the authorisation needed to undertake the investigation
- the nature of the possible outcome of the investigation, and
- the reporting obligations of the decision-maker(s).

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.

When gathering evidence following a cyber-security incident, it is important that it is gathered in an appropriate manner and that its integrity is maintained. In addition, if ASD is requested to assist with investigations, no actions which could affect the integrity of evidence should be carried out before ASD becomes involved.

Case Study – ANAO Audit Administration of Security Incidents, Including the Conduct of Security Investigations

The audit found that entities can encounter a wide range of security incidents including the theft or loss of assets, the inappropriate handling or suspected compromise of classified information, instances of unauthorised access to information or restricted work areas and the physical or threatened assault of staff. The number and type of security incidents generally reflects the nature of each entity's work, including the level of classified information. It may also be influenced by factors such as the conduct of regular security inspections, the strength of security awareness among staff, and the ease of reporting security incidents.

The audit also found that the majority of security incidents (recorded by the audited entities) related to matters that did not warrant a formal investigation. For example, many security incidents were of a minor or procedural

[2] Noting that under the Notifiable Data Breach scheme a data breach likely to result in serious harm to any of the individuals to whom the information relates requires an objective assessment. Refer to guidance material on identifying eligible data breaches.

nature and were dealt with by local managers or supervisors taking remedial action, or were addressed through the conduct of routine inquiries.

Minor security incidents were generally addressed by less formal mechanisms, such as procedural inquiries, and more serious incidents were the subject of formal investigation. In some cases, preliminary investigations were conducted if, for example, all the details or the extent of the impact of a security incident were not known before deciding whether or not to conduct a formal investigation.

Recommended Approaches

- Where security investigation functions are shared across entity work areas or with an outsourced service provider, the CSO, CSIO (or another delegated SES officer) maintain oversight of the investigation and establish mechanisms to monitor the investigation and ensure communication of issues, findings and decisions to all relevant parties.
- When conducting a security investigation, evidence is gathered in a manner that ensures the integrity of the evidence is maintained.

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 and be given an opportunity to be heard by an unbiased decision-maker and respond. 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.

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.

See PSPF Guidelines Section 19.7 and PSPF Release 2024 (Section 19.7) for further guidance on procedural fairness.

3.7.2 Security Investigation Process

A security investigation establishes the facts about the security incident, including:

- who, what, why, when, where and how
- the nature of the incident and how it occurred
- the circumstances that led to the incident occurring
- the person/s involved
- the degree of damage to security interests, government people, information or assets, and
- procedural or system improvements needed to prevent or reduce the likelihood of recurrence

The steps for managing security investigations are:

- appoint an investigator
- develop an investigation plan
- gather and record evidence
- prepare final report
- action recommendations or findings, and
- close investigation.

3.7.2.1. Appoint Investigator

In the interests of procedural fairness, it is important that the investigator be impartial and not have an actual or apparent conflict of interest in the matter being investigated.

Entities are strongly encouraged to provide relevant and appropriate training for investigators, as determined by the entity. The AGIS provides guidance on recommended training or qualifications for investigators. Where insufficient power to collect available or required evidence is identified, or if a conflict of interest is identified, the investigator is encouraged to refer the investigation to another person or entity with the necessary powers.

An investigator's key responsibilities include:

- understanding the incident being investigated and the terms of reference
- identifying the relevant law, policy or procedures that apply
- making sufficient inquiries to ascertain all relevant facts
- ascertaining whether an offence or incident has occurred based on the relevant facts
- reporting the findings, identifying the reasons for the findings, and
- making relevant recommendations.

An investigator also assesses:

- applicable legislation that may determine the nature of and set the framework for the investigation
- the nature of the incident
- how serious the incident is and therefore the possible level of harm it has for the entity, or more widely, for the Government
- whether the incident indicates the existence of a systemic problem
- whether it is part of a pattern of conduct, and
- whether it may breach any Australian law, especially any criminal provision.

3.7.2.2. Develop an Investigation Plan

The investigation plan identifies:

- the terms of reference for the investigation
- the issues to be investigated
- any relevant legislation, particular provisions of a code of conduct, entity policy and procedures, particular standards and guidelines

- required evidence
- methods and avenues to collect the evidence
- legal requirements and procedures to be followed in collecting evidence
- the allocation of tasks, resources and timings, and
- arrangements in case the terms of reference or investigation plan need to be modified during the investigation.

The terms of reference for the security investigation could include:

- the background
- resources allocated (people, finances and time)
- timeframes
- types of inquiries to be conducted
- extent and limit of powers of the investigating officer (consistent with relevant Commonwealth and jurisdictional legislation) during the investigation to collect evidence by:
  - obtaining information from people about policies, procedures and practices
  - accessing relevant records and other material
  - interviewing witnesses and suspects
  - undertaking search and surveillance activities
- the format of progress reporting and the final report, and
- any special requirements or factors specific to the investigation.

Recommended Approach

- ✔ CSO approve the terms of reference, objectives and limits for all security investigations.
- ✔ CSO seeks regular progress reports on active investigations.

3.7.2.3. Gather, Record and Store Evidence

The investigator identifies, collects and presents information or evidence that goes to proving or disproving any matters of fact relating to an incident. In an investigation, the types of evidence are:

- physical
- documentary (records)
- verbal (recollections)
- expert (technical advice).

Evidence gathered in a security investigation may not comply with the rules of evidence and therefore may not be satisfactory in a criminal investigation, or where legal proceedings might arise in relation to the incident. For guidance on obtaining, recording and storing evidence, refer to AGIS.

If ASD is requested to assist with investigations, no actions which could affect the integrity of evidence should be carried out before ASD becomes involved.

Recommended Approaches

- A separate and complete file is maintained by the investigator for each investigation that documents dates and times of all discussions, phone calls and interviews, and captures decisions and conclusions made during the course of the investigation.
- This file, and any physical evidence, is stored securely to prevent unauthorised access, damage or alteration, and to maintain confidentiality and continuity of the evidence. It is important that the record includes the handling of physical evidence and any tampering with the file or physical evidence.

3.7.2.4. Prepare Final Report

At the conclusion of the investigation, the investigator presents the findings report to the CSO, CISO, commissioning body (e.g. security governance committee) or decision-maker. The report details reasons for the findings according to the terms of reference using supporting material, and provides recommendations that could include:

- disciplinary action
- dismissal of a disciplinary charge following a constituted hearing
- referral of a matter to an external entity for further investigation or prosecution, and
- changes to administrative or security policies, procedures or practices.

In drawing conclusions regarding administrative investigations, whether conducted for security or other reasons such as disciplinary purposes, the decision-maker needs to be satisfied that the allegations are proven 'on the balance of probability'.

3.7.2.5. Close Investigation

The investigation is considered closed when all reports are completed and evidence is documented and filed. It is better practice for an independent person, preferably more experienced than the investigator, to review the closed investigation. This allows an impartial assessment of the investigation that may identify improvements to investigation practices.

3.7.3 Criminal Investigations

A Commonwealth criminal offence refers to an act that will generally be an offence under the *Crimes Act 1914* or the *Criminal Code Act 1995* or other Commonwealth legislation.

The purpose of a criminal investigation is gathering admissible evidence which may lead to placing the offender/s before the court.

As outlined in the AGIS, if a security matter is considered by the entity to be a serious crime or complex criminal investigation, it must be referred to the AFP in accordance with the AFP referral process (see www.afp.gov.au), except where:

- the entity has the capacity and appropriate skills and resources needed to investigate serious crime or conduct complex criminal investigations and meet the requirements of the Commonwealth Director of Public Prosecutions in gathering evidence and preparing briefs of evidence, or
- the issue involves alleged breaches of the *Commonwealth Electoral Act 1918*.

Where another entity has legislative investigative powers (e.g. Comcare and ASIO), that entity may have primacy in determining which type of investigation takes precedence.

Where a suspected Commonwealth criminal offence is not or cannot be referred to the AFP for investigation (see AFP website), or requires initial investigation prior to establishing a need to refer to the AFP, entities may need to conduct an investigation for matters such as suspected fraud, theft and unauthorised disclosure of official information. To the extent possible, when investigating a suspected Commonwealth criminal event or a matter that may result in a criminal investigation, entities are encouraged to consider the rules of evidence.

The rules of evidence cover:

- admissibility of evidence: whether or not the evidence can be used in court, and
- the weight of evidence: the quality and completeness of the evidence.

For guidance on obtaining, recording and storing evidence in accordance with the rules of evidence, refer to the Australian Government Investigations Standards (AGIS).

See ISM's Guidelines for cyber incidents for further guidance on integrity of evidence for cyber investigations.

The Commonwealth Fraud Control Framework sets out procedures for investigating actual or suspected fraud against the Commonwealth.

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 that aggregates the annual reporting data for the Minister for Home Affairs, Minister for Immigration and Multicultural Affairs, and Minister for Cyber Security.
    - The consolidated report will not name entities or provide entity-specific results.
    - The consolidated report will be provided to entities and be published on the PSPF website for public transparency.
- PSPF Classified Assessment Report – provides the Government with entity-specific results and provides a heat map of protective security issues and vulnerabilities.
    - The classified report will name entities not meeting the requirements and standards of the PSPF.
    - The classified report will not be made publicly available nor be provided to entities.

As per PSPF Requirement 0031 and PSPF Requirement 0032, Entities are required to report under the PSPF to provide assurance about their implementation of sound and responsible protective security practices, and to identify security risks and vulnerabilities, and the steps being taken to mitigate them. See PSPF Guidelines Section 4.2 for guidance on the Annual Protective Security Report process.

All non-corporate Commonwealth entities must meet the PSPF requirements, consistent with the requirement in section 21 of the *Public Governance, Performance and Accountability Act 2013* for the Accountable Authority of a non-corporate Commonwealth entity to govern the entity in a way that is 'not inconsistent with' the PSPF.

Corporate Commonwealth entities and Commonwealth companies that implement the PSPF are also encouraged to report on their security compliance.

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.

The 2024-25 PSPF Reporting Pack will detail information on the new reporting process, calculation methodology and provide useful information to support the annual reporting process.

4.2.1 Reporting to Ministers

PSPF Requirement 0031 mandates the entity's annual protective security report is provided to the entity's minister.

The Accountable Authority is responsible to their Minister for the protective security of their entity's people resources and activities, and must provide their Minister with an annual protective security report. This should be provided no later than December. This report provides the Minister with assurance that entity is

implementing sound and responsible protective security practices and demonstrating year on year efforts to improve the entity's security capability and posture.

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).

The annual protective security report also provides the Accountable Authority, CSO and CISO with a clear picture of the entity's protective security posture, highlights areas for improvement, what is currently preventing full compliance, and any action that is required to achieve full compliance.

The 2024-25 PSPF Reporting Pack will include more detail on what information should be provided to the Minister(s).

4.2.2 Reporting to the Department of Home Affairs

PSPF Requirement 0033 mandates the Accountable Authority approves and verifies the entity's annual protective security report content and PSPF Requirement 0032 ensures the report is submitted to the Department of Home Affairs.

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

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

The PSPF Offline Reporting Template is a Microsoft Excel template that is updated each reporting period to support entities that are required to report above PROTECTED. For information on submitting on SECRET and TOP SECRET systems, contact the Government Protective Security Policy Section on PSPF@homeaffairs.gov.au

The Department uses the annual reporting data to prepare two reports to Government. See PSPF Guidelines Section 4.1—Security Reporting to Government for details.

4.2.2.1. Protective Security Reporting Process

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.

Table 13: Overview of Annual Reporting Process

Stage	Details
Notification	The entity's nominated Submitter (this is the CSO by default but can be delegated by the CSO to another officer) is the key contact for the entity's PSPF annual report and is responsible for commencing and submitting the assessment in the PSPF Reporting Portal. The appointed Submitter will receive an email from the PSPF Reporting Portal at the commencement of the reporting period advising that the reporting period is open and available for them to commence their entity's report.

Stage	Details
Commencement	The Submitter will then have 48 hours to commence the entity's assessment in the PSPF Reporting Portal by: Step 1: Acknowledging and accepting the reporting obligations Step 2: Selecting the security classification of the data to be entered into the portal: • PROTECTED/OFFICIAL: Sensitive – allows entity to report online through the portal. • SECRET/TOP SECRET – provided the entity with an offline reporting template for completion offline and submission via commensurate system Step 3: Assign the role of 'User Administrator' to at least one user. User Administrator's privileges allow them to manage users associated to the entity's profile. The Submitter can make other changes to portal users if desired, however this can also be done by the User Administrator. Step 4: Select the 'Create Assessment' button. The entity can then populate the report.
Completion	Once the entity has populated the report, the Submitter is required to: • Confirm the final security classification of the information populated in the report. • Confirm that the CSO (and CISO where relevant) has approved the report. • Confirm that the Accountable Authority has verified the accuracy of the report and approved the reported, including the date the Accountable Authority approved it. • Confirm the entity will be provided to the Minister and Portfolio Minister.
Submission	The 'Submit Assessment' button will only appear one all components of the report are completed. Only the Submitter will see this button. Once clicked, the assessment is available for the Department of Home Affairs to review. Once submitted, the entity is no longer able to amend their report.
Finalisation	The Department of Home Affairs reviews the entity's report and then either: • Returns to the entity for remedial action (and the Submitter will need to make the necessary amendments and then follow the 'completion' and 'submission' stages again). • Refers the report to the PSPF Assurance Team, or • Finalises the report in the PSPF Reporting Portal to conclude the entity's annual reporting obligations. Once finalised, the report cannot be reopened.

Protective Security Reporting Categories and Sub Categories

PSPF requirements will either be designated as 'Compliance' or 'Yes/No' requirements. Compliance requirements will have three reporting categories:

- Fully implemented
- Risk managed
- Not yet implemented

From these categories, the entity selects the category that best reflects their level of implementation for the corresponding requirement. Entities will only fit into one response category for each requirement, thereby removing the need to make 'self-assess' which level of maturity best applies.

PSPF requirements are mandatory and must be fully implemented. However, in entities are not penalised for employing a 'risk-managed' approach to implementation but are required to:

- provide a summary of what prevented full implementation of the requirement, and

- upload a risk management plan detailing arrangements for managing the requirement, approved by the Accountable Authority.

The plan must be uploaded to proceed, otherwise a different reporting response ('Fully implemented' or 'Not yet implemented') must be selected.

Entities only need to confirm that the Accountable Authority has approved the risk management plan for the requirement. Entities should retain a copy of the Accountable Authority's approval in case they are asked to provide evidence as part of assurance or scrutiny activities.

Each category will have sub-category options. Entities will select the sub-category that best describes the primary driver for selecting that category. Entities may select up to two sub-categories for each category. These sub-category options will be expanded or amended as required over time.

The examples provided in Figure 3 and Figure 4 are prototypes only. These arrangement are dependent on upgrades to the PSPF Reporting Portal and are subject to change.

The 2024-25 PSPF Reporting Pack will detail the PSPF Risk-Based Compliance Reporting arrangements, including the calculation methodology and a copy of the Risk Management Plan Template that entities will be required to use when selecting the 'risk managed' category.

Figure 3: Example of Reporting Question

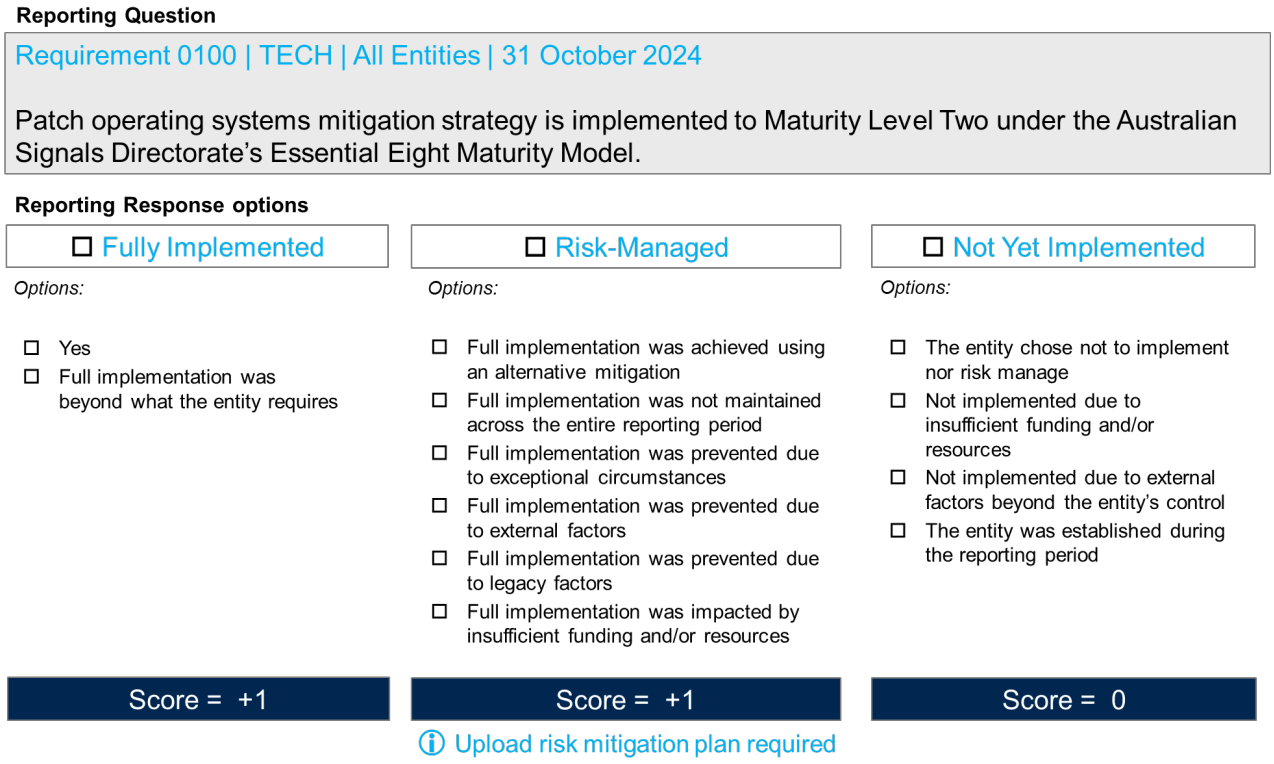
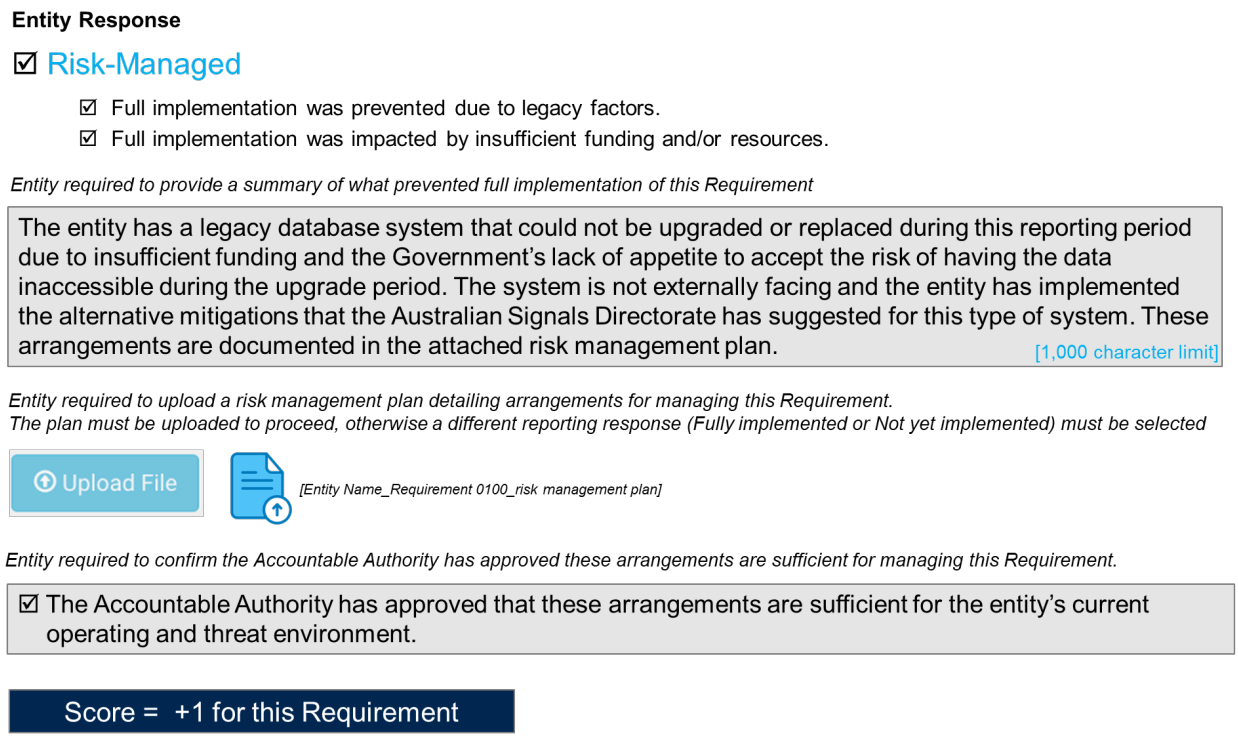


Figure 4: Example of Risk-Managed Response



4.2.2.1.1. Preparing for the Annual Reporting Process

PSPF Requirement 0022 mandates that entities must develop, establish and implement security monitoring arrangements to identify the effectiveness of the entity's security plan and establish a continuous cycle of improvement.

The entity prepares for the annual reporting process by assessing their effectiveness in:

- overall security capability, posture and culture
  - identify and manage security risks
  - minimise the harm to government people, information and resources
  - respond to and learn from security incidents and investigations
- achieving the security goals and objectives identified in the entity's security plan
  - strategies and timeframes identified during the year (or in the previous year) to improve the entity's security position
- level of implementation of each PSPF Requirement across the six domains,
  - adequacy of any arrangements in place to 'risk manage' PSPF requirements where full implementation is prevented.

The Department of Home Affairs will distribute a PSPF Reporting Information Pack and hold a PSPF Reporting Forum to help entities prepare for the annual reporting process.

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 previous reporting period. The PSPF Reporting Portal is accredited to process, store and communicate information up to PROTECTED.

All Commonwealth entities have access to the PSPF Reporting Portal. Contact PSPF@homeaffairs.gov.au for assistance with access.

VANguard Federated Authentication Service

Entities must be federated with VANguard in order to access the PSPF Reporting Portal.

VANguard is a secure authentication service provided free of charge to government entities by the Department of Industry, Science and Resources VANguard | Department of Industry Science and Resources. VANguard allows authorised portal users to access the PSPF Reporting Portal using their existing network login, without the need to re-enter a password to access the Portal.

PSPF Reporting Portal Roles

There are a number of roles in the PSPF Reporting Portal and guides on these roles are available to government personnel on the Protective Security Policy GovTEAMS community.

- Submitter – is the key contact for the entity's PSPF annual protective security report and is responsible for commencing and submitting the assessment in the PSPF Reporting Portal.
    - The entity's nominated Submitter is the CSO by default. The CSO may delegate this role to another suitable officer.
    - The Submitter role can only be assigned by the Government Protective Security Policy section in the Department of Home Affairs. Contact PSPF@homeaffairs.gov.au to request.
    - The Submitter will receive an email from the PSPF Reporting Portal at the commencement of the reporting period advising that the reporting period is open and available for them to commence their entity's report.
    - See PSPF Reporting Portal – Submitter Role (available on GovTEAMS) for further details.
- User Administrator – is responsible for managing the entity's portal users, including adding removing users and assigning roles other than the Submitter role.
    - The Submitter assigns the role of User Administrator to a suitable user. The Submitter may elect to assign the role of User Administrator to more than one user.
    - User Administrator privileges do not automatically include the 'Security Incident Reporter' or 'Contributor' roles. If these roles are required, the Submitter needs to assign them to the User Administrator.
    - See PSPF Reporting Portal – User Administrator Role (available on GovTEAMS) for further details.
- Security Incident Reporter – allows the user to report a significant security incident to the Department of Home Affairs on behalf of their entity.
    - The User Administrator assigns the Security Incident Reporter role to suitable users.
- Contributor – this role allows a portal user to participate in the annual protective security reporting process. The Contributor role also gives the user access to any security incidents reported through the PSPF Reporting Portal.
    - The User Administrator assigns the Contributor role to suitable users.

- Contributors can either be granted:
  - full access with the 'Contributor (All Modules)' which allows them to see and edit all content other than sections that are restricted for other user roles, or
  - restricted access to specific modules 'Contributor (Module X)' which allows them to see and edit only the modules that have been granted access to.

- **Read Only** – this role allows a user to supervise, but not edit, the information entered during the reporting period. Contributor access overrides the Read Only restrictions.
  - The User Administrator assigns the Read Only role to suitable users.
  - Read Only users can either be granted:
    - 'Read Only (All Modules)' which allows them to view all content, or
    - restricted access to specific modules 'Read Only (Module X)' which allows them to view only the modules that have been granted access to.

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 posture 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.

The assurance function will be established in the Government Protective Security Policy Section in 2025 and will support entities with improving their implementation of PSPF requirements and accuracy of reporting, it will not be an auditing function.

The 2024-25 PSPF Reporting Pack will detail further details on the assurance function and activities.

4.2.2.4 Sharing of Annual Security Reports

The annual PSPF reporting data is shared with:

- ASD 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.
- ASIO to support its efforts to uplift government security capability.
- Australian National Audit Office (ANAO) 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

PSPF Requirement 0035 mandates that entities complete and submit the annual Cyber Security Survey to ASD.

ASD is the Technical Advisory Entity responsible for cyber security. See PSPF Guidelines Section 1.3.

ASD issues the annual Cyber Security Survey directly to entities. This Survey is technical in nature and complements the cyber security questions asked in the PSPF reporting process. Entities are required to confirm they have met this reporting obligation to ASD in the annual protective security report to the Department of Home Affairs. Entities that do not meet this reporting obligations will be identified in the PSPF Classified Assessment Report to Government.

ASD uses the data gathered in Cyber Security Survey to prepare the Commonwealth Cyber Security Posture Report to inform the Australian Parliament on the implementation of cyber security measures across the Australian Government.

Part Two

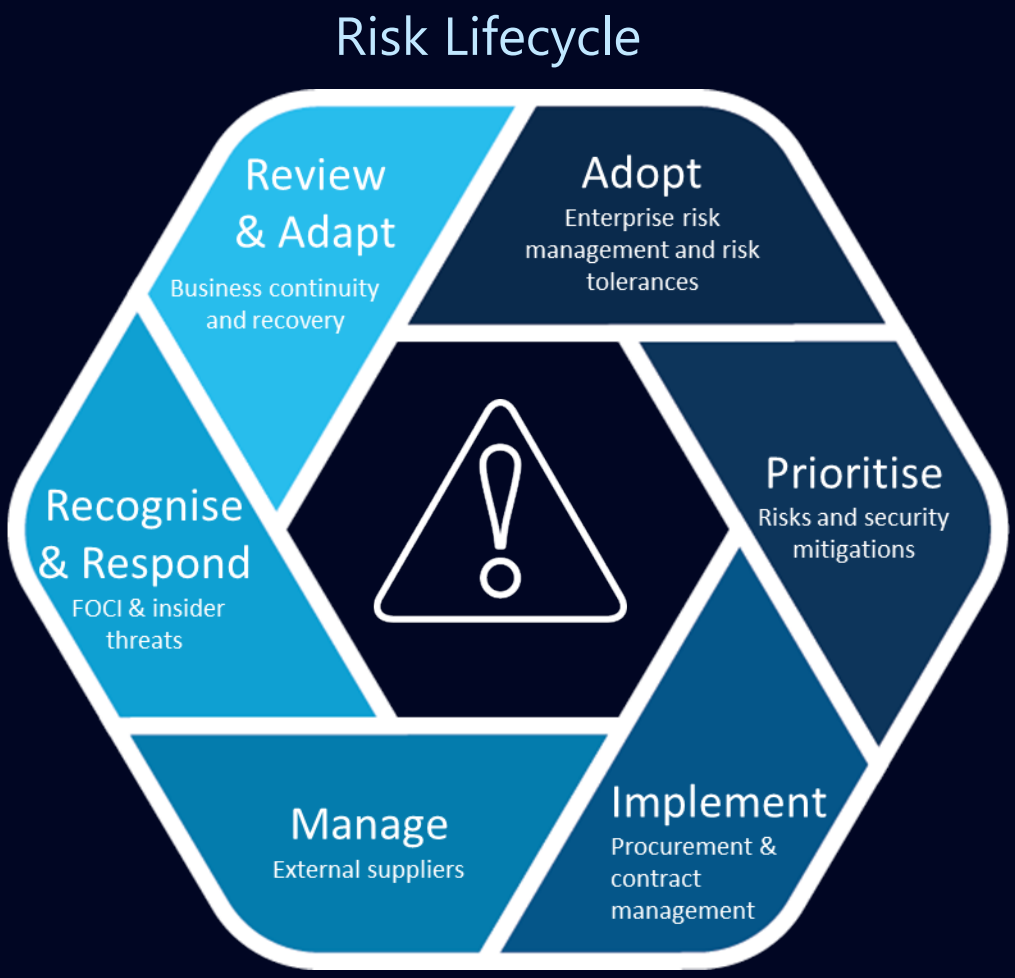
Risk

Security Risk Management

Third Party Risk Management

Countering Foreign Interference and Espionage

Contingency Planning



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.

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.

Security risk management includes identifying, assessing and prioritising risks to people, information and resources. It involves the efficient and coordinated application of protections that minimise, monitor and control the probability and effects of risks.

Security risk culture is the entity's system of values and its personnel's behaviours, attitudes and understanding that are related to security risk that shapes the risk decisions of the entity leadership and personnel. Having a mature risk culture is a fundamental enabler of security risk management and good government business.

An entity with an effective security risk culture is one where the leadership team and personnel:

- comprehensively understand security risks
- appropriately manage security risks in their operational environments
- prioritise security risk management in their everyday practices
- make informed decisions on risks within agreed entity security risk tolerances, and
- react and respond to changes in the security risk environment.

The success of security risk management depends on the effectiveness of security planning and how well arrangements are supported by the entity's senior leadership and integrated into business processes. This includes meeting requirements of the PSPF or adopting mitigations that are equivalent to or exceed those requirements.

Effective security risk management supports better decision-making and builds positive risk culture by:

- identifying possible risks and opportunities in advance, lessening the potential of adverse outcomes and increasing the likelihood of desirable outcomes
- having processes in place to monitor risks and provide access to reliable, up-to-date information about risks
- providing guidance around appropriate limits through well understood risk appetite and risk tolerance statements
- providing transparency over the decision-making process and the achievement of entity objectives.

When security risk management is effectively implemented it supports robust resilience through a positive risk culture and it allows entities to identify, quantify, and make coordinated and informed decisions in managing and mitigating their security risks. It also allows entities to proactively identify opportunities to learn from past issues through meaningful training and support across all levels of management.

See the Department of Finance's Developing a positive risk culture information sheet, Commonwealth Risk Management Policy Elements Eight – Maintaining risk management capability and Four – Embedding systematic risk management into business processes.

5.1 Security Risk Tolerance

PSPF Requirement 0036 mandates that the security plan must detail the entity's tolerance to security risks, agreed by the Accountable Authority. 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, and the level of risk the Accountable Authority is willing or able to accept.

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 requirements and standards to achieve its objectives.

Risk tolerance is an informed decision to accept a risk. It is the level of acceptable risk after risk treatment to achieve an objective or manage a category of risk. Determining whether a risk is acceptable involves judgment. It is highly dependent on the entity context and the Accountable Authority's approach.

Risk tolerance is based on the principle of managing risk to a level that is as low as reasonably practicable, allowing for flexible and innovative business practices. It is a practical application of risk appetite, which is the amount of risk an entity is willing to accept or retain within its tolerance levels and the limits of PSPF requirements.

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 tolerances.

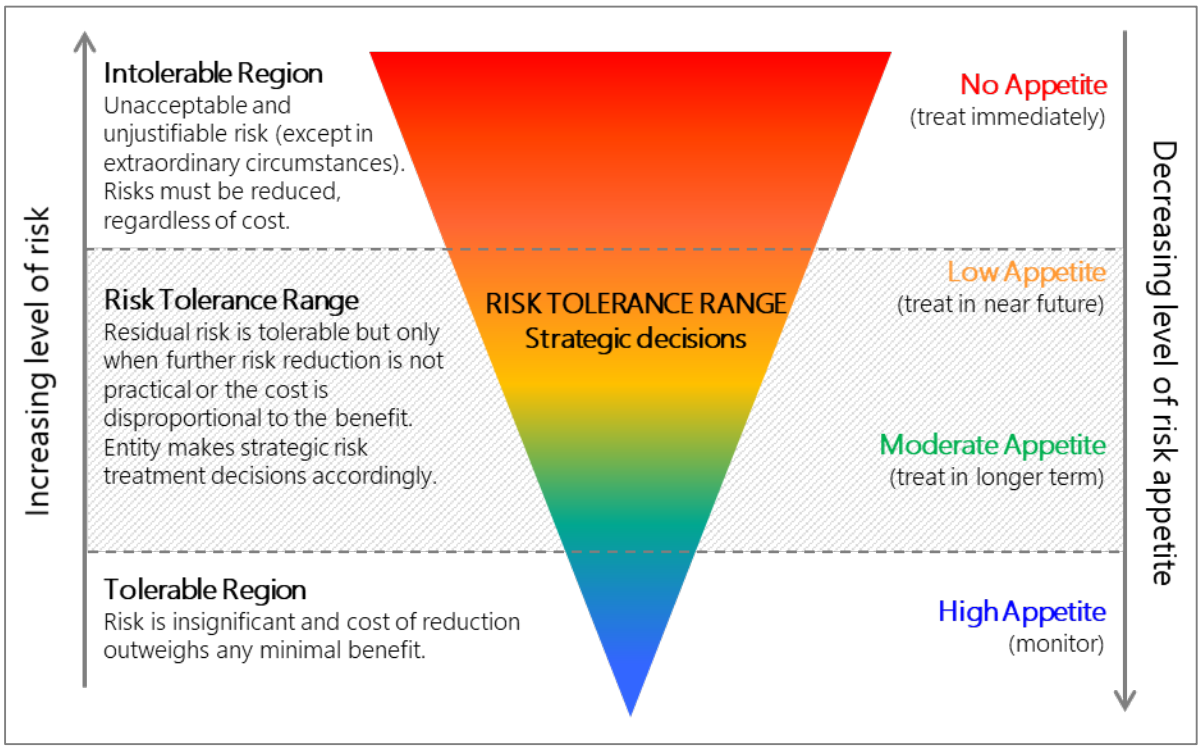
An entity's risk tolerance can be affected by changes in evaluation criteria and the Accountable Authority's (or the Government's) appetite for risk. It can vary depending on:

- prevailing political and community sensitivities and expectations
- the nature of a security incident (e.g. terrorist act, hacking)
- existing or emerging security incidents (e.g. trusted insider, cyber-attacks)
- strategic or business priorities
- vigilance, resilience and adaptability of personnel and how effective they are at applying security awareness principles
- resource availability for treatment, and
- the ability of the government, entity or individual to absorb losses.

Manipulating risk assessment inputs (consequence or likelihood of a risk) to achieve a lower result is not an appropriate method of risk management and bypasses the intent of risk tolerance. Entities are encouraged to develop appropriate rating scales for likelihood and consequence in accordance with their risk tolerances.

In most cases, determining risk tolerance and levels of risk appetite can be understood as a gradient scale, where the appetite for the risk becomes progressively less tolerable as the risk level increases (see Figure 5).

Figure 5: Risk Tolerance Regions



For information see the Department of Finance's Understanding Risk Appetite and Tolerance risk management policy factsheet.

Recommended Approaches

- Accountable Authority documents the entity's protections to reduce, treat or mitigate risks, including the defined benchmarks against which the success of implemented risk mitigations are measured.

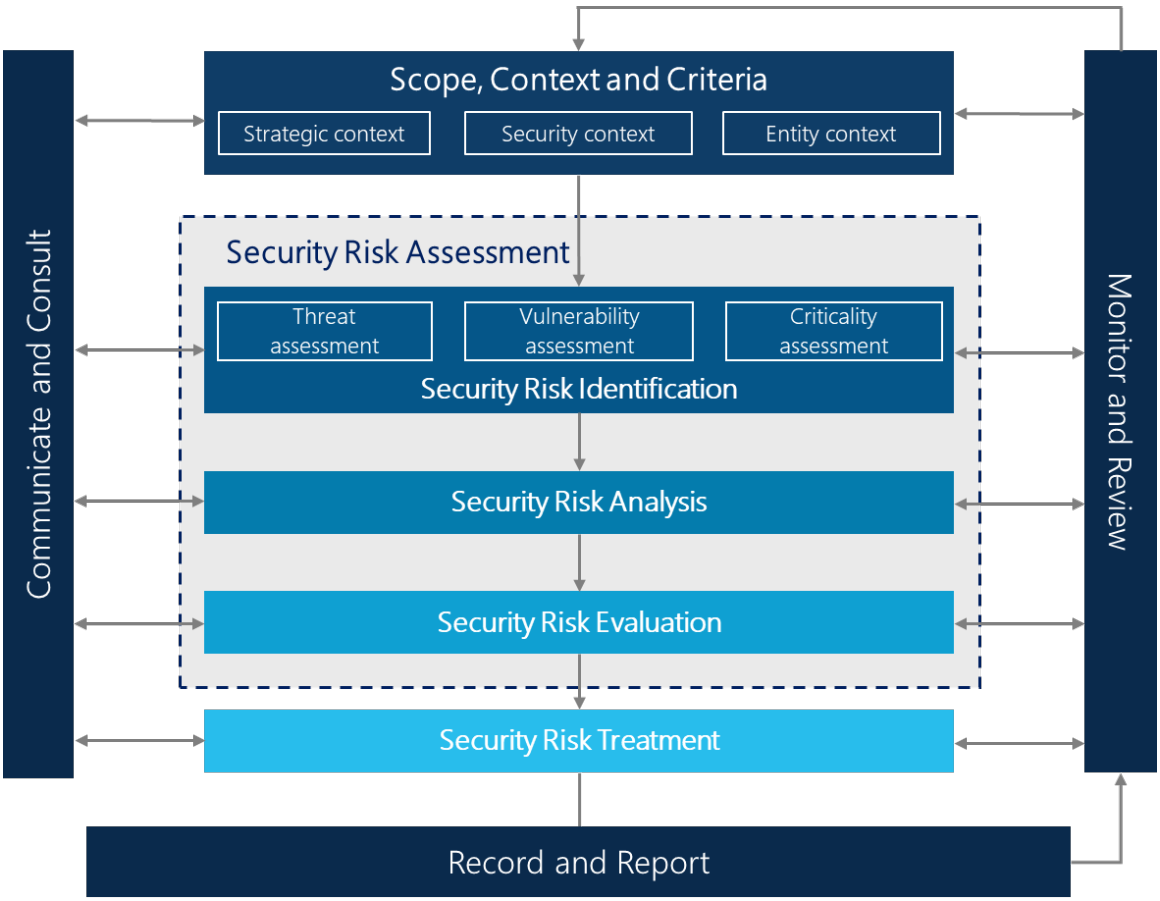
5.2 Security Risk Management Process

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

The key elements of the security risk management process are:

- establish the context
- security risk assessment
- security risk treatment
- communicate and consult
- monitor and review, and
- record and report

Figure 6: Security Risk Management Process



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 and safety and environmental goals, and can apply at multiple levels such as strategic, organisation-wide, project, product and process levels.

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

Recommended Approaches

- Consider where security risks intersect with other risks including fraud, privacy and business continuity.
- Treat risk holistically across the entity's operations and identify opportunities to treat multiple risks with one mitigation control.

5.2.2 Shared Security Risk

PSPF Requirement 0037 mandates that a risk steward (or manager) is identified and responsible for each security risk or category of security risk, including for shared risks.

Element Six of the Commonwealth Risk Management Policy mandates that entities must collaborate to management shared risks. The policy defines a shared security risk as those risks extending beyond a single entity which require a collaborative effort of shared oversight and management. This include security risks that extend across entities and may involve external stakeholders, other sectors and jurisdictions. In large, complex entities, shared risk can exist within the entity as well as between them.

The management of shared risks involves:

- security risk assessment to determine the appropriate protective security measures for the combined shared risks
- identification of accountability and responsibility for the management of these risks and accepted by those best positioned to manage them
- agreement by all parties involved, and
- applying additional controls where risks are shared between parties with differing risk tolerances.

See Element 6: Shared Risks | Department of Finance for further guidance and case studies.

Recommended Approaches

- ✔ Consider where security risks intersect with other risks including fraud, privacy and business continuity.
- ✔ Security risks arising from co-tenancy or shared facilities are addressed by applying protective security policy.
- ✔ Security risks associated with a particular location (e.g. physical boundaries, crowded public space, government precinct) where there is no identifiable other party to share the assessment and management of the risk, the entity mitigates the risk to the extent it is able to within its operations

5.2.3 Scope, Context and Criteria

The first step is to establish the scope, context and criteria. This step aligns the security risk management approach to the entity's objectives and unique operating environment.

Define the scope of your security risk management activities, the objectives and outcomes that need to be made, what tools and resources will be required, and how these activities connect to the entity's other enterprise risk management activities.

Next consider the internal, external and security context of your security risk management activities. Entities should consider the entity-specific context, external context and security context.

Internal context includes:

- scope and parameters of activities where risk management is applied
- resources (or limitations) available or required for risk treatments and activities
- reputational expectations or objectives
- logistical or locational challenges
- outcomes of related internal or external audit reports
- security risk management processes adopted, and
- processes for documenting results of risk assessments and risk treatments.

External context includes:

- regulatory environment, including legislative or policy obligations and responsibilities, foreign laws or potential jurisdictional access to information
- political or economic climate, and
- community sensitivities or expectations.

Security context includes:

- purpose and scope of security in supporting or achieving the entity's business objectives
- criteria for evaluating the significance of security risks
- risk appetite and tolerance criteria and threshold levels for the entity
- threat and risk environment (areas of concern, specific threats identified, known vulnerabilities)
- decision-makers (when and by whom)
- critical asset statement (what are you looking to protect)
- interdependencies and links to other plans or security procedures
- details of any shared risk, and
- constraints and assumptions.

Establishing the context also involves identifying the relevant stakeholders, including external parties that may expose the entity to risk, or are already exposed to an entity's risks, or may be able to help an entity manage risk.

Examples of key stakeholders are:

- service providers and managed service providers
- government partners (including other Commonwealth entities or state and territory agencies)
- non-government partners, for example academic institutions, and
- international government partners.

Establishing a criteria for security risks informs decisions to consider, or not consider, risks in the context of your entity's objectives.

5.2.4 Security Risk Assessment

Security risk assessment is the process of risk identification, analysis and evaluation to understand the risks, their causes, consequences and probabilities. The aim is to generate a comprehensive list of threats and risks that affect the protection of the entity's people, information and resources and identify the sources, exposure and potential consequences of these threats and risks. Consideration is also given to the entity's prevailing and emerging risk environment.

Security risk assessment involves:

- security risk identification
- security risk analysis, and
- security risk evaluation.

Each risk should be described as comprehensively as possible, so that decision-makers can fully understand the position. This may be in the style of a formal assessment undertaken by competent personnel, or a contracted service provider.

5.2.4.1. Risk Identification

Identifying security risks generates a clear, comprehensive and concise list of potential sources of risk and threats (referred to as a risk register, see example below) that could impact government, entity operations or continuous delivery of services.

This is achieved by mapping the sources of risk (threat assessment), determining the importance of organisational assets (criticality of assets) and the manner in which these elements may facilitate or inhibit this interaction (vulnerability).

- Threat Assessment – identifies the source of harm and is used to inform the entity's risk assessment. Threats are assessed by determining the intent to cause harm, damage or disruption and the capability (the potential that exists to actually cause harm or carry out intentions) of the threat source. In preparing a list of security risks, consider such questions as:
    - What could happen? (potential event or incident and resulting outcomes or consequences)
    - What is the likely outcome and impact of the risk eventuating?
    - When could it happen? (how frequently)
    - Where could it happen? (physical location and assets affected)
    - How could it happen? (sources, potential threats, catalysts, triggers)
    - How reliable is the information that the risk assessment is based upon?
    - Why could it happen? (causes, underlying factors, vulnerabilities or inadequacies in protective security controls or mitigations)
    - Who could be involved or effected? (individuals or groups, stakeholders or service providers)
    - Do entity mitigation measures or activities create risk to clients or the public?

Table 14: Risk Register Example

Item	Description
Description	Describe the risk (consider the questions above)
Category	People, information, property, reputation, financial, business operations
Event	Occurrence or change of a particular set of circumstances
Source	Threat or hazard that is the source of the risk
Cause	Why the threat or hazard is a risk
Consequences	Level of impact the risk will have on the entity
Risk criteria	Determined tolerability against consequence and likelihood tables
Priority	Comparing the level of risk (magnitude of risk = consequence + likelihood) with the risk criteria
Controls	Adequacy of existing controls in place, or the known controls for the risk
Current risk rating	What is the current risk rating status

Item	Description
Risk decision	Does the risk need treatment
Treatments	What action needs to be taken, by whom, with what resources and by when
Residual risk rating	Once treatments have been implemented, what will be the residual risk rating
Stakeholders	Who else is impacted by the risk (e.g. other entities, contractors, service providers)
Previous risk information	Information on any previous risk, threat or vulnerability assessments

- Criticality Assessment – identifies and assigns importance to entity people, information and resources that are critical to the ongoing operation of the entity or to the national interest. Asset identification and security risk management documents can form part of the security plan or be standalone and inform the security plan.
    - Criticality assessment will be different depending on the entity's purpose, business objectives and risk environment. Criticality assessments include:
    - Criticality ratings – the scale of the resources' importance to the entity (e.g. a numerical scale 1-5 or importance value scale such as catastrophic, significant, moderate, low, insignificant). Alternatively, a business impact level can be applied by assessing the impact on the entity if the integrity or availability of the resource was compromised (applying a business impact level to the confidentiality of a resource means applying a security classification.
    - Consequence of loss, compromise or harm – a description of what the consequence is.
    - Category – consequences can also be expressed across categories such as people, information, property, reputation, financial, business operations or services.
- Vulnerability Assessment – identifies the degree of susceptibility and resilience of an entity to hazards. To understand the potential of risks, it is recommended that entities assess the possible vulnerabilities to each risk to gauge the consequence and likelihood of these risks. This process of understanding possible vulnerabilities helps entities to prioritise the risks and guides the allocation of resources in mitigating their effects.

5.2.4.2. Security Risk Analysis

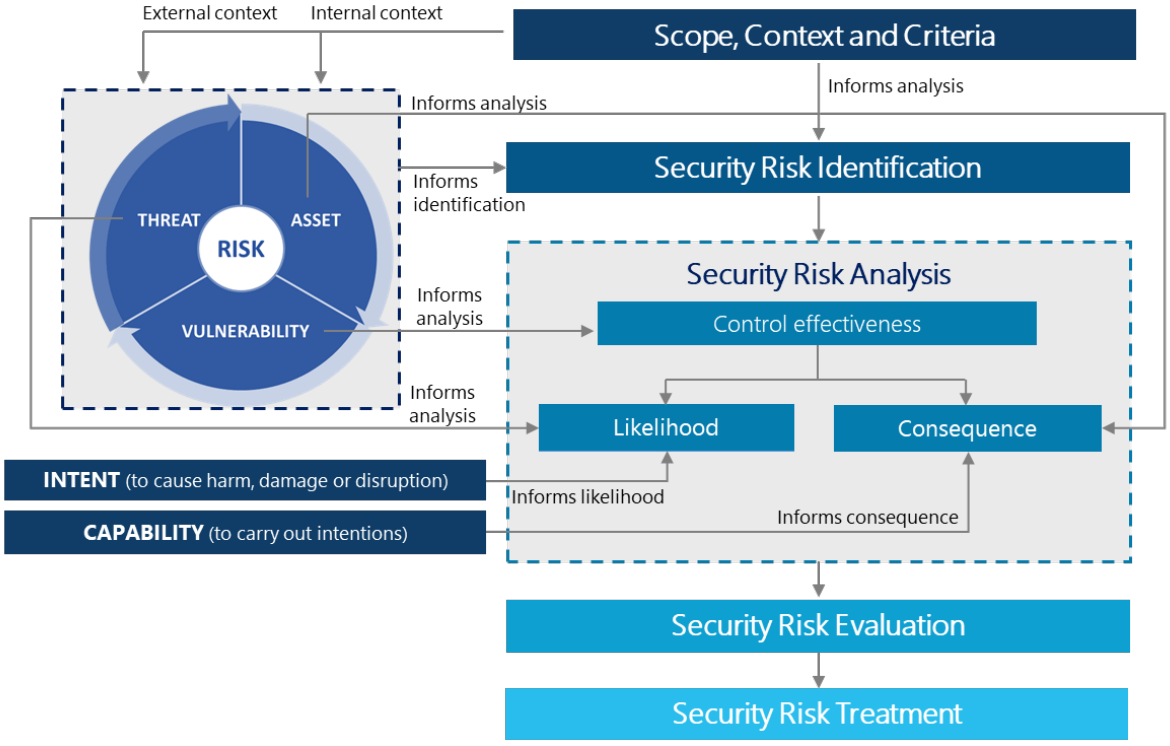
Risk analysis involves assessing the likelihood and potential consequence of each identified risk, determining the level of risk rating and assessing whether additional controls are required.

Aims of risk analysis:

- Determine control effectiveness – whether the existing control measures are adequate or effective in managing identified risks.
- Define the likelihood and consequence of the event. This is achieved by considering the:
    - Likelihood – the chance or probability of the event occurring, or the probability or frequency of the event (an occurrence or change in a particular set of circumstances, it can be one or more occurrences and can have several causes) occurring.
    - Consequence – the outcome affecting objectives if the event occurs (consequences can be expressed qualitatively or quantitatively and can be certain or uncertain, and have positive or negative effects on objectives). There may be a number of possible outcomes associated with an event.

- Assign the level of risk rating based on the likelihood and consequence risk matrix. The overall risk rating is determined by combining the likelihood and consequence estimations. Risk rating allows the security risk to be prioritised in order of decreasing risk levels. This helps with deciding the tolerability of risk in the evaluation step.
- Prioritise risks for subsequent evaluation of tolerance or the need for further treatment.
- Provide an improved understanding of the vulnerability of critical assets to identified risks.

Figure 7: Using Threat, Criticality and Vulnerability to Inform Risk Analysis



5.2.4.3. Security Risk Evaluation

Risk evaluation involves making decisions based on the outcomes of risk analysis about whether risks are:

- acceptable (tolerable) with existing controls or further treatment (risks identified as acceptable or tolerable with no further treatment still need to be documented, monitored and periodically reviewed to ensure they remain acceptable), or
- unacceptable (intolerable) and need treatments (consideration is given to the criteria for determining tolerability).

See PSPF Guidelines Section 3.1.3.3—Element: Risk Tolerance.

5.2.5 Security Risk Treatment

Appropriate risk mitigation treatments and controls are selected to address identified security risks in accordance with the entity's security plan objectives. Efforts to treat security risks will not remove them completely but aim to reduce them to a more tolerable level.

Risk treatments can be applied separately or in combination. It may not be possible or cost-effective to implement all possible risk treatments. However, it is necessary to choose, prioritise and implement the most appropriate treatment or combination of treatments.

Australian Standards HB 167: Security Risk Management outlines strategies for risk treatment.

This includes a six-step process where entities:

- prioritise intolerable risks
- establish treatment options
- identify and develop treatment options
- evaluate treatment options
- detail design and review of chosen options, including the management of residual risks, and
- communicate and implement.

Treatment plans:

- prioritise the risks to be treated
- assess current risk; the actual risk once all treatments have been implemented
- identify gaps and residual risks that remain or require further treatment
- capture decisions about treatments and actions to be taken to address or treat identified security risks
- determine appropriate timeframes to implement treatment or when further consideration of mitigations is required be considered
- identify resources, budget allocations, timeframes (defined and measurable) and responsibilities to achieve required treatment outcomes, and
- establish monitoring and reviewing processes.

Examples of risk treatment strategies include:

- Accept the risk, where:
    - based on judgment or informed decision, the risk is considered to be tolerable (either before or after treatment)
    - the only option is to retain the risk and continue to monitor it until the circumstances change and action can be taken
    - taking on increased risk in order to pursue an opportunity where the benefit outweighs the risk, or
    - the risk may be considered intolerable but due to capability, resources or exceptional circumstances may be accepted.
- Avoid the risk,[3] by:
    - deciding not to start an activity that gives rise to the risk, or
    - removing or reducing the activities or personnel, including contractors, that create the exposure.

[3] Where entities have been directed to undertake the activity, they will not be able to avoid the risks. Risk treatment is preferable to risk aversion or avoidance.

- Exploit the risk, by taking or increasing the risk in order to realise the benefit that an opportunity affords by ensuring the event occurs.
- Reduce the risk, by changing the likelihood or consequence (or both) by:
  - implementing new treatments or controls to reduce, deter, delay or detect the threat or event
  - improving business processes, training or practices, or
  - establishing or improving audit and compliance arrangements, contractual arrangements, or communication channels.
- Share the risk, where:
  - the risk has no single owner but is shared with another party or parties (e.g. through shared services, entities co-located in the same building, inter-entity taskforce, partnership or joint venture), or
  - the risk may have no apparent owner.

See PSPF Guidelines Section 5.2.2—Shared Security Risk.

Recommended Approaches

- ✔ When selecting treatment, the entity balances the cost and effort of implementing the treatment with the expected benefits and ensure the treatment is proportional to the determined risk rating level.
- ✔ Adopt a risk-rating-matrix approach for determining the levels of risk.

5.2.5.1. Implementation

Implementation involves deciding on the resources required and who is responsible for implementing the risk treatments. In addition, implementation details the ongoing resources needed to maintain the required level of protective security and identifies resources that may be needed to take additional precautions if the threat level increases.

5.2.6 Communicate and Consult

Communication and consultation with stakeholders, contracted service providers and decision-makers throughout all stages of the process is an essential element of the security risk management process. This approach ensures stakeholders are properly represented, have their views taken into account in determining risk criteria and confirms that all participants understand their roles and responsibilities.

It is recommended that the following is documented:

- audience and stakeholders
- communication objectives and activities (what are you trying to achieve, how it will be achieved, delivery method, expectations), and
- monitoring and review processes (noting that communication and consultation occurs at all stages of the security risk management process).

See the Department of Finance's Risk Management Process for advice on attributes of good risk communication.

PSPF Requirement 0038 mandates that 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.

Sharing information between entities may help to mitigate threats across government. For example, parties that pose security threats, such as organised crime groups, may target multiple government entities.

Particular consideration is required where decisions have adverse implications for another entity, including under shared service arrangements, or where the supported entity has a different risk tolerance level or limited capacity to meet the resulting obligations.

Entities are strongly encouraged to adopt a default position to seek and share information (unless security, secrecy or privacy limitations are in place). In the event these limitations are in place, entities are encouraged to look at options that allow partial sharing of information. Where there are legislative limitations, such as under the *Privacy Act 1988*, entities may consider using formal agreements with other entities to share information.

See PSPF Guidelines Chapter 12—Information Sharing.

5.2.7 Monitor and Review

Security risk management requires monitoring to ensure the entity is able to adapt or respond to incidents and changes in their threat or risk environment, prevent further exposure to hazards, maintain a positive risk culture and deliver against the PSPF.

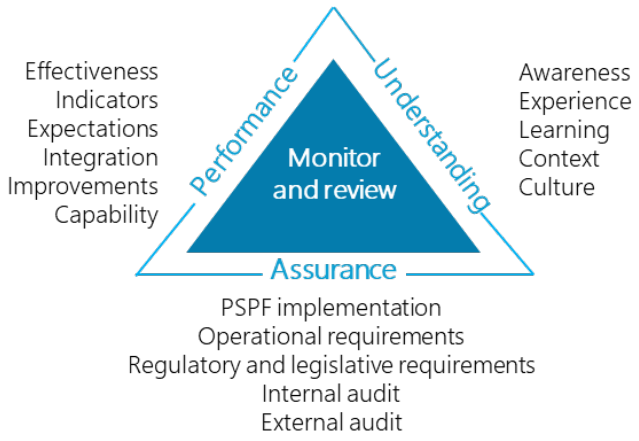
Decisions to implement risk treatments should be recorded but this is not the end of the risk management cycle. The cycle is continuous. Reviewing the external and internal environments and reconsidering the context allows the entity to determine how effectively their protective security controls and measures are performing and how they are achieving the objectives.

Key questions to ask when monitoring and reviewing risk may include:

- Are the controls (and respective implementation strategies) effective in minimising the risks; how might improvements be made?
- Are the controls comparatively efficient and cost-effective?
- Are the assumptions made about the context/environment still valid?
- Do controls comply with policy requirements, legal obligations and entity procedures?
- Is the entity's security planning approach effective in managing security risks and achieving objectives?

Australian Standards HB 167: 2006 Security Risk Management Chapter 8 outlines strategies for monitoring and review, including the model detailed in Figure 8.

Figure 8: Monitoring and Reviewing Security Performance



5.2.8 Record and Report

The security risk management process is most effective when well documented and shared. The final stage of the security risk management process is recording and reporting on decisions, security risk management activities and performance. This enhances decision-making, internal governance and monitoring arrangements, and interactions with key stakeholders, and will inform the entity's annual protective security reporting.

Recording and reporting aims to ensure that all relevant entity stakeholders have an informed understanding of the entity's security risks, security risk management processes and the outcomes from the implementation of the security risk treatments through effective communication.

The information provided during the year by recording the security risk management processes feeds directly into the entity's security risk reporting.

Reporting is a conduit that allows an entity to continuously improve their security risk management process by feeding back into the start of the process. The information included in an entity's reporting helps verify that the security risk assessment is adequately identifying, analysing and evaluating security risks, and helps inform decision making.

Reporting also acts as a form of record keeping that details the rationale behind the decisions made during the security risk management process.

For reporting to be effective, strong governance is required from the entity, in the form of detailed processes and procedures for reporting obligations. The report should also be reviewed by the entity's Accountable Authority.

Entities should ensure that their reports provide information in a clear manner to prevent ambiguity or misinterpretations. The security risk reporting should also be tailored to strategic requirements of the entity.

Entities should consider the following factors when developing their security reports:

- what information needs to be provided
- the relevance of the information to an entity's strategic goals
- who the intended audience and stakeholders of the report are, and
- the frequency of reports.

An entity's security report should include the following:

- the scope and objectives of report
- the overall security risk status of the entity
- details on the effectiveness or ineffectiveness of the entity's implemented security risk treatment
- the most critical security risks and how they apply to the entity
- any changes to the security risk management process since the last report, and
- conclusions and recommendations.

6 Third Party Risk Management

6.1 Procurement, Outsourcing and Contract Management

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.

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.

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 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 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.

Relevant Commonwealth Procurement Rules[4]

- Relevant entities must establish processes to identify, analyse, allocate and treat risk when conducting a procurement. The effort directed to risk assessment and management should be commensurate with the scale, scope and risk of the procurement. Relevant entities should consider risks and their potential impact when making decisions relating to value for money assessments, approvals of proposals to spend relevant money and the terms of the contract.
- Relevant entities should consider and manage their procurement security risk, including in relation to cyber security risk, in accordance with the Australian Government's Protective Security Policy Framework.

6.1.1 Procurement of Outsourced Services

PSPF Requirement 0039 mandates that 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.

A key determinant of value for money in procurement activities is achieving quality security outcomes. 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.

Each entity is accountable for the security risks arising from its procurement of goods and services. However, goods and service providers can also play an important part in identifying and addressing security risks. The Commonwealth Procurement Rules state that risks are most effectively borne by the

[4] Commonwealth Procurement Rules paragraphs 8.2-8.3

party best placed to manage them. As such, if an entity is best placed to manage a particular risk, it would be inappropriate to transfer that risk to the supplier.

The Commonwealth Procurement Rules state that risk is required to be considered in all procurements. Entities are encouraged to specifically consider and manage any associated protective security risks. This includes:

- identifying mandatory and desirable security requirements in procurement request documents, including any specific provisions relating to subcontracting
- using relevant protective security terms and conditions in procurement contracts
- managing the ongoing delivery of security requirements for contracted goods and service providers, and
- implementing appropriate security arrangements at the completion or termination of contracts.

Understanding the relevant threats and vulnerabilities associated with a procurement helps entities identify suitable security treatments. For example, procuring cloud technologies may appear a more affordable and faster alternative to other technology solutions. However, it could require specific contract clauses and operational controls to mitigate risks associated with storing information in a foreign country.

If identified security risks cannot be mitigated to an acceptable level or the security risks to government are too great, entities should seek alternative procurement arrangements and maintain a record of such decisions.

A risk assessment identifies the protective security risks associated with the procurement and informs decisions on whether these risks are acceptable or unacceptable. This assessment should consider (at a minimum):

- national interest
- risks to critical infrastructure
- risks to those transacting with the entity through a contracted provider
- the ability to manage and control resources in an outsourced, offshore or supply-chain arrangement with potentially changing legal frameworks
- foreign involvement and the potential for foreign ownership, control or interference
- the insider threat
- informing associated entities of relevant risks, relevant treatments and the likely effects where there are multiple government stakeholders, and
- security plans as a ready source of information on risks to entity information.

See PSPF Guidelines Section 5.2.4—Security Risk Assessment and Section 5.2.4.1—Risk Identification.

Table 15: Examples of Potential Procurement Security Risks

Type	Description
Foreign involvement	Outsourcing can be cost-effective for providing goods or services. However, it can also affect an entity's risk profile and control over its threat environment. Entering into an arrangement where resources are made or held offshore (either by the contracted provider or a subcontractor) can have additional risks. For example, services located offshore are subject to the laws of those countries and may be subject to lawful and covert collection.

Type	Description
	The nature of the legal powers to access, or restrict access, to government resources held in foreign countries may differ. See Section 6.1.3—Foreign Ownership, Control or Influence in Procurement.
Differences in the business and legal cultures in other nations	The difference in the business and legal cultures in other countries may give rise to additional risks, affecting the confidentiality, availability and integrity of Australian Government resources. For example: • the tolerance (legal and law enforcement effectiveness) and acceptance of corruption and crime differ across countries • foreign enterprises owned, influenced or funded by foreign governments, or • a lack of visibility into the suppliers' corporate structures, funding or use of non-reciprocating safe harbours. Similarly, the extrajudicial behaviour of foreign governments and the ability of citizens to refuse those demands may be limited, potentially giving rise to further risks that need consideration. A lack of effective rule of law may encourage attempts to misappropriate information or assets (including by organised crime).
Complications arising from the simultaneous application of multiple legal jurisdictions	Complications may arise from information being subject to the laws of multiple jurisdictions This may occur in circumstances where: • foreign laws apply to a supplier because it is located offshore, sometimes in multiple locations • foreign laws have an extra-territorial application to a supplier located in Australia as well as abroad, or • the goods or services provided by the supplier pass through a foreign jurisdiction. Most foreign jurisdictions have legislative powers that allow access to assets, communications and stored information for the purposes of law enforcement and national security. In some cases, these laws allow international law enforcement and national security agencies to access information and resources held overseas or in Australia. Any qualified assurances and controls provided by the supplier will need to align with entity risk profiles to ensure that information and resources are managed securely.
Complications from multiple delivery entities/ contractors (supply chain)	In some cases, an entity may engage multiple providers to deliver goods or services, or a contracted provider may engage multiple subcontractors as part of a supply chain. Engagement of multiple partners inherently increases the complexity, and associated security risks, of a procurement. In addition, transparency of (and control over) operations is more challenging the further down a supply chain it is from government. Consider security risks of each contracted provider independently and holistically across all contracted and subcontracted partners. Look to reduce vulnerabilities and ensure security continuity to manage risks along the whole supply chain. See Section 6.2.2—Supply Chain Risk Management.
Insider threat	Australia is exposed to persistent and sophisticated exploitation. Allowing access to entity resources can diminish an entity's mitigation of threats. The incentives and capability to conduct malicious insider activity may be exacerbated by: • Increased motivation o Australia is an attractive target for exploitation due to its prominent role in the Asia-Pacific region, its strong diplomatic, defence and intelligence relationship with the United States, its resource industries and expertise in research and development fields. o Entity resources (particularly exploited information or assets) could be used to gain economic, diplomatic or political advantage against Australia. For example, stolen intellectual property can be used to gain access to new technologies while circumventing costly and lengthy research and

Type	Description
	development programs. Personal information (such as financial or medical records) could be used for malicious activities through social engineering. o State-sponsored actors working on behalf of a foreign entity are sophisticated and active malicious adversaries. They seek national security information to identify vulnerabilities or gain advantage and often target Australia's commercial sectors (e.g. resources, banking and telecommunications). • Ease of acquiring capability o Technical capability is increasingly sophisticated with malicious tools, information and supporting guidance readily available. The ease of acquiring capability, coupled with the potential high gains (e.g. financial, economic, diplomatic or political) may entice malicious activity by insiders (and others). • New technologies generating new vulnerabilities o Technological advancements (such as the growth in cloud computing and mobile devices like smartphones, laptops and tablets) generate platforms with distinct software, settings and applications. A greater number of trusted insiders using new technologies may increase vulnerability to exploitation. See Section 7.3—Insider Threat Programs.

Contact the ASIO Outreach for assistance managing national security risks.
Contact the Cyber and Infrastructure Security Centre for assistance in managing critical infrastructure risks.

Recommended Approach

- ✔ Consult experienced subject matter experts as part of the risk assessment process, when warranted by the scale, scope and nature of the security risks involved in the procurement.

6.1.1.1. Protective Security Terms and Conditions

PSPF Requirement 0040 mandates that 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 standards, and to avoid exposing the entity or the Australian Government to an unacceptable level of risk.

Meeting this requirement involves specifying terms and conditions in procurement documents (such as requests for tender and subsequent contracts) that:

- detail the specific PSPF Requirement numbers that the provider is expected to meet across the six security domains, as mandated in PSPF Requirement 0041
- identified security risks relevant to the procurement, and
- establish clear obligations to report security incidents and changes in circumstances that are relevant to the contract or the entity's security arrangements, as mandated in PSPF Requirement 0042, and
- impose responsibilities for the ongoing management of security matters.

Written contracts between two or more parties outline each party's rights and obligations. One of the benefits of having a contract identifying relevant security terms and conditions is that these terms and conditions are legally enforceable.

For guidance materials and templates to assist in developing legally binding agreements (such as contracts or deeds), an entity may wish to:

- seek legal advice
- contact the Department of Finance for policy advice in relation to general procurement in government via procurementagencyadvice@finance.gov.au and refer to Commonwealth Procurement and the Commonwealth Contracting Suite for further information, or
- contact the Digital Transformation Agency (DTA) at ictprocurement@dta.gov.au for information about IT procurement in government and for access to the IT Procurement Portal in DTA.

Table 16: Examples of security contract terms and conditions

Context	Security Terms and Conditions
General	The PSPF defines personnel as employees and contractors, including secondees and any service providers that an entity engages. It also includes anyone who is given access to Australian Government resources held by the entity as part of entity sharing initiatives. Contracts therefore need to impose equivalent protective security conditions of engagement, access requirements and ongoing security obligations to ensure the protection of the entity's people, information and resources.
Governance	Governance matters to considering covering in contracts: • providing for periodic updating of security requirements to accommodate changes in the: o risks to the entity or contracted provider o National Terrorism Threat Level, and o Australian Government's protective security policies (including the current PSPF Release and ISM) • taking into account national security provisions (for example, removing information from a data centre if ownership is transferred to a foreign owner) • conditions that the contracted provider immediately notify the contracting entity where they become aware of: o a proposal to acquire the business o an actual change in the provider's ownership, and o where a substantial overseas investor (including foreign government investors) acquires a substantial interest (e.g. equal to or greater than 20 per cent) of the contracted provider • require the contracted provider to notify the entity of any actual or suspected security incidents that may impact on the entity's information which is held by or in transit to/from the provider, or their ability to deliver the goods or services they have been contracted to provide. Also require the contracted provider to: o report any breaches of IT or technology security to the entity and, where relevant, ASD,[5] and o report IT or technology security issues to the contracting entity even when not immediately relevant to the contract. • permitting the entity to terminate the contract if the contracted provider fails to comply with the protective security provisions in the contract, including unwillingness or inability to remedy any security breaches • including strategies for transition security arrangements at the completion or termination of the contract: o requiring that information (both electronic and hard copy) and assets be returned, and deletion of all entity's information from the contracted provider's

[5] To report a cyber security incident, ASD can be contacted on for critical infrastructure and big business: 1300 172 499, or for individuals and SMEs: 02 6141 6666

Context	Security Terms and Conditions
	IT/technology systems (for information classified at PROTECTED or above, sanitising their IT/technology systems in accordance with the ISM), and o requiring the contracted provider to maintain protective security measures if for legal reasons they cannot return records or assets at the end of a contract.
Personnel security	Personnel security matters to considering covering in contracts: • assurances of confidentiality and for non-disclosure of official information (including security classified information) to a third party • requiring the contractor to sign a non-disclosure agreement in situations where a security clearance is not required[6] • including a requirement for the contracted provider to seek written consent from the entity, to provide access to the entity's information or resources by their personnel, and • setting standards of behaviour which the contractor's employees are expected to observe, including code of conduct and the application of protective security measures.
Sponsoring security clearances	It is not uncommon for contracted providers to work for a number of government entities at the same time. In such circumstances it can be challenging to identify the relevant entity to sponsor security clearances for the contractor's personnel. Sponsorship should be provided by the entity that: • first engaged the contractor where a security clearance is required • requires the highest level of security clearance, or • is the lead entity for the contract that covers multiple entities (for example as a result of a panel arrangement).
Ongoing suitability	Ongoing suitability matters to consider covering in contracts: • provisions requiring the contracted provider to prevent all access to security classified material by the contractor's personnel whose security clearances are revoked, lapsed or who no longer require access • requirement for the contracted provider to report to the entity when any of the contractor's personnel have had any incidental or accidental contact with security classified material • arrangements for dealing with any reportable changes in circumstances and the reporting and investigation of security incidents or breaches. For example if a contractor's personnel: o is employed on other concurrent contract/s with other entities or governments o has been expelled from an accrediting body o has been arrested or is undergoing disciplinary proceedings, or o has been dismissed, has resigned or is on long-term leave • ongoing security awareness training that includes the contractor providing training for its personnel to: o protect the entity's assets and information o report changes in personal circumstances, and o report suspicious, ongoing, unusual or persistent contact.
Separation	Separation matters to considering covering in contracts: • provisions for revoking physical and technology system access upon a contracted provider's personnel's exit from the company

[6] Signing a non-disclosure agreement is not suitable in certain circumstances, for example, when sharing information with foreign nationals, or when Australia is not the originator.

Context	Security Terms and Conditions
	• an obligation on the contracted provider to advise the entity when the provider's personnel (or subcontractors) with sponsored clearances have ceased to work on the entity's contract, and • requiring the contracted provider to remind current and departing personnel who have accessed official or security classified information that the confidentiality requirements are perpetual, not time-specific.
Information security	Information security matters to consider covering in contracts: • specifying that resources provided by the entity, or generated as a result of the contract, belong to the government and are not used for any purpose other than the goods or services covered by the contract • a direction to disclose any potential conflict of interest that would impact on security in the performance of services on behalf of the Australian Government • conditions addressing any potential for legal rights which may be held by a third party over the contracted provider, that could allow access to entity information • a direction that no service that requires access to official information (including security classified information) be subsequently subcontracted to a different agreed provider, without written approval by the contracting entity, and • a direction that where the contracted provider knows or suspects that any security classified information relating to the contract has been, or is likely to be, transferred overseas without approval in writing, it must promptly provide details to the contracting entity and follow reasonable directions from the entity in relation to the matter.
Physical security	Physical security matters to considering covering in contracts: • ensuring the contracted provider's premises and facilities used to handle or store security classified information meet the PSPF's physical security standards to protect information and resources up to, and including, the nominated security classification level, and • allowing entity representatives to access the contracted provider's premises, records and equipment to monitor the contracted provider's compliance with protective security conditions.

Case study – Contractor Personnel Security

An entity considers using cleaning services from a cleaning company as opposed to directly employing cleaners. The cleaning company employs Australian and non-Australian citizens.

Cleaners will have access to secure physical zones and may have contact with security classified information up to and including the PROTECTED classification level.

The entity includes contract conditions requiring the provider to adhere to requirements for appropriate access to classified resources. This includes taking steps to obtain the required security clearance for ongoing access to security classified information such as where contact exceeds the maximum allowable limit of three months temporary access over a 12 month period. Contract conditions also require the provider to report instances where uncleared contracted cleaners have contact with security classified material, this assists the entity to monitor security incidents.

Case study – Contractors Handling Security Classified Information

An entity, in its role as a regulatory authority, outsources services to an external consultancy to assess and confirm the financial income, assets and expenditure of a third-party entity as part of the annual compliance process. This process involves transmission and sharing of OFFICIAL: Sensitive information between the entity and the outsourced service provider. The entity ensures tender documentation and contracts include clauses stating what and how the information is to be shared, transferred, stored and disposed of.

6.1.1.2. Outsourced Services provided by Government Entities

PSPF Requirement 0043 mandates that 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 approach 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.

See Infosec Registered Assessors Program (IRAP) | Cyber.gov.au.

6.1.2 Ongoing Management of Security in Contracts

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

It is important for each entity to establish a robust governance and assurance process to ensure contracted providers implement the applicable protective security requirements and meet the security obligations specified in the contract. These may include:

- applying relevant personnel security provisions such as security clearance vetting requirements for people accessing classified Australian Government resources (applying the same security measures to contracted provider personnel as an entity would to its employees)
- applying relevant information handling controls and storage arrangements to protect security classified information (requiring contracted goods and service providers to protect Australian Government information resources in the same manner as an entity would)
- applying relevant physical security measures for protection at facilities where government resources are held and facilities where goods are prepared for government use, as well as addressing all hazards an entity may face in the protection of its people, information and resources (including requiring contracted goods and service providers to apply protection against national security threats).
- establishing governance arrangements to manage ongoing protective security requirements (during the contract work stage and at the completion or termination of the contract). This includes permissions for entities to:
    - amend or terminate a contract where issues of national interest arise (e.g. procedures to address actual or suspected security incidents or breaches, or the supplier has changed ownership without notifying the entity or seeking approval)
    - monitor ongoing contracts (e.g. access to premises, records and equipment) through all levels of subcontracted supply chains
    - manage changes to the provision of goods or services, and
    - terminate the contract if the provider fails to comply with provisions in the contract, including where there is an unwillingness or inability to remedy or mitigate security incidents.
- assurances that the 'primary' contracted provider:
    - immediately directly notify the entity of actual or suspected security incidents and follow direction from the entity in relation to incident investigations, including providing assistance to rectify the situation. Where entities jointly hold personal information (such as an entity and contracted provider), both entities have obligations to notify the OAIC and affected

individuals in the event of an eligible data breach. For guidance on managing these obligations, see Data breaches involving more than one organisation

- take reasonable steps to prevent, detect and respond to fraud and corruption
- implement security arrangements to manage risks corresponding to the material and/or property provided by the entity (including personnel, information and physical security measures required to protect the material and property at all times from unauthorised access, misuse, loss, interference, unauthorised modification and unauthorised disclosure)
- periodically review its security arrangements under the contract to ensure the arrangements are current, and address the risks and any changes in the security environment
- is responsible for managing and monitoring the protective security of its subcontractors, including supply-chain arrangements, and
- is providing timely, accurate and complete information on changes to the ownership and control of its subcontractors where required.

Recommended Approach

- ✔ Identify who is accountable for each security treatment or control in the contract.

6.1.2.1. Monitor and Review Contracts

PSPF Requirement 0044 mandates that 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.

Changes in the entity's risks, as well as its internal and external security environment, may necessitate a flexible approach to contracts and their management.

Consider the following questions when monitoring and reviewing contracts:

- Has a positive working relationship been established with the contracted provider to promote open communication? Are issues being identified and resolved in a prompt manner?
- Is the contracted provider advising employees (including subcontracted providers and their personnel) of the protective security conditions that apply under the contract?
- Have the premises been inspected prior by a delegate of the CSO/CISO to the commencement of the contract to verify that protective security measures specified in the contract comply with the PSPF? Has there been periodic reinspecting of contracted providers' and subcontractors' premises during the life of the contract, specifically:
  - prior to re-negotiation or extension of a contract, and
  - following a security incident at the provider's or subcontractor's premises?
- Have the ongoing clearance maintenance requirements been managed for a provider's staff holding security clearances?

- Where the contracted provider processes or stores entity information (and requires access to that information), have the provider's information security procedures been tested and monitored through regular site visits and audits? (i.e. use of third-party audits, including certifications)[7]
- Has the contracted provider monitored the security of information in systems that store, process or communicate entity information through, for example:
    - conducting vulnerability assessments
    - maintaining change and release management processes
    - testing their business continuity plan, or
    - identifying, reporting and containing any cyber security incidents that could affect entity information?[8]
- To reduce information being lost, destroyed, damaged, compromised or misused, has the contracted provider maintained authorisations for access to information only when the following conditions are met:
    - the person has the required level of security clearance
    - there is a genuine need-to-know the information
    - access will comply with legislative and policy requirements
    - there is no conflict of interest regarding the information, and
    - the person has completed a declaration of secrecy?

Case Study: Potential Data Centre Ownership Changes

An entity outsources its data holdings to a managed service provider. While the provider's data facility is physically located in Australia, the entity identifies a potential risk of foreign ownership, control or influence.

To help mitigate the identified security risks, the entity includes conditions in the contract regarding changes in ownership and management. Mitigations of foreign interference risks include:

- requiring advice on any ownership changes (including of subsidiaries), or changes to ownership structure, operational management and day-to-day control, and contracting arrangements for companies with access to the data facility
- permission to cancel or amend the contract, remove servers and data or associated equipment, recover records (or maintain protective security measures if records cannot be returned) without penalty if there is a change in ownership or management
- requiring Australian citizenship for the service provider's operational managers
- ensuring co-located services with the service provider have no technical access to the entity's data, or
- requiring no offshore control or access to infrastructure, systems and entity data.

During the life of the contract, the cloud facility is subsequently sold to a foreign investor. Security provisions in the contract allow the entity to discontinue use of the data centre when ownership changed.

[7] For information on certification, see Infosec Registered Assessors Program (IRAP) | Cyber.gov.au
[8] For information on technology system security, see the ISM

Recommended Approaches

- Evaluate compliance with contract conditions by performing ongoing assessments (such as regular inspection of premises used to store Australian Government information or resources, or an ongoing accreditation program).
- Identify a contract manager who is responsible for monitoring and reviewing risk for each contract can assist in this process.

6.1.2.2. Manage Security Incidents in Contracts

A security incident may have wide-ranging and critical consequences for the entity and the Australian Government. Investigation of security incidents (actual or suspected) provides valuable information for future risk reviews and assessments. This helps entities evaluate current security plans and procedures.

Oversight of incidents through timely and thorough reporting is important during the life of the contract. This allows entities to adjust security procedures and contract conditions if necessary, to mitigate any security risks exposed by an investigation and to implement any additional safeguards to avoid further security incidents from occurring. For example, in service contracts there may be downtime experienced during a cyber-incident response. This may affect performance measures associated with the contract. To address this, contract terms may be structured to encourage appropriate responses to security incidents.

PSPF Requirement 0042 mandates that 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. This includes ensuring that the provider notifies the entity in a timely manner

This requirement relates to any security incident that may affect:

- the provider's ability to deliver the goods or services they have been contracted to provide
- the ability of the contracted provider's personnel to hold a security clearance, and
- any entity resources that are held by, or are in transit to and from the contracted provider.

Entities may require contracted providers to report security issues even when not immediately relevant to the contract. Where an entity suffers an eligible data breach (including where it jointly holds personal information with a third party such as a contracted provider), notification obligations arise under the OAIC Notifiable Data Breaches scheme. A data breach incident may also trigger reporting obligations outside of the Privacy Act.

6.1.2.3. Complete or Terminate Contracts

PSPF Requirement 0045 mandates that contractual terms and conditions include appropriate security arrangements for the completion or termination of the contract. This helps to safeguard government resources and limit the potential of security classified information being compromised.

This obligations includes to:

- recover records (both electronic and hard copy) and resources under the control of the provider (or require the contracted provider to maintain protective security measures if for legal reasons the provider cannot return records or assets at the end of the contract)

- require the provider to delete all entity information from the provider's IT/technology systems (additionally, for information classified at PROTECTED or above, the ISM details controls for sanitising technology systems)[9]
- complete obligations for separating personnel as a Sponsoring Entity, for example:
    - for personnel with security clearances, inform the Authorised Vetting Agency of the separation of contracted provider's personnel,[10], and
    - obtain formal acknowledgement from contracted providers and their personnel of their continuing obligations to maintain confidentiality.

See the Department of Finance's Commonwealth Procurement Rules for information regarding setting contract end dates and termination options.

6.1.3 Foreign Ownership, Control or Influence in Procurement

PSPF Requirement 0046 mandates that when making procurement and contract decisions entities 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.

An organisation is considered to be operating under Foreign Ownership, Control or Influence (FOCI) when a foreign interest has the power, direct or indirect, to direct or decide matters affecting the management or operations of that entity. FOCI is considered to be interest, whether or not exercised, and whether or not exercisable, through the ownership of the company under the purview of its National Security Authority/Designated Security Authority. This can be by contractual arrangements or by other means. FOCI can mean an entity operates 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.

Providers subject to FOCI can be directed to act against their own business interests, and to undermine the security of their products and services, provide entities not included in the contract to have privileged access to systems, or provide sensitive data. FOCI risk is one of many security risks entities need to consider when considering contract providers for procurement purposes.

Every time an entity interacts with an external provider, there is an inherent risk. If an external provider (or their products or services) is granted access to valuable systems, allowed to operate with privileged access, or has control over a large portion of a supply chain, they may represent a weakness that could be exploited by malicious actors. If there is no ongoing access or maintenance by the provider, or it is not internet-connected, then the risk of FOCI would be lower, or potentially non-existent.

International agreements and arrangements can include provisions for classified contracts. Before an entity engages a foreign contractor on a classified contract, it is important that an international agreement or

[9] For OFFICIAL information stored on cloud-based services, a similarly stringent approach to sanitisation may be warranted. For example, in a multi-national cloud-based company there may not be a practical way to erase physical media. In such cases a suitable solution may be stronger encryption of hosted content.
[10] This will cease the entities' sponsorship of security clearances for the contracted provider's personnel. Where entities advise the Authorised Vetting Agency that a contractor no longer requires a security clearance, the Authorised Vetting Authority will inform other known entities using the contractor. This gives interested parties the opportunity to assume sponsorship, including the responsibilities for clearance maintenance of the contractor.

arrangement is in place if the contract involves sharing classified information or assets. See PSPF Guidelines Section 12.3—International Information Sharing.

6.1.3.1. Identify Potential FOCI Risks

First identify whether the provider the entity is seeking to engage is operating under, or has the potential to be compromised by, FOCI.

Indicators of FOCI risk fall broadly into three categories:

- Jurisdictional – refers to the legal authority that a foreign government exercises over its citizens and businesses, regardless of their location. FOCI can be inferred where the business or third-party service, by nature of its operations or international presence, is compelled to provide a foreign government with access to private Australian Government resources (i.e. data, intellectual property, sensitive materials) without the knowledge and/or consent of the Australian Government.
- Corporate Governance – Corporate Governance risk refers to where the business is subject to state ownership or control structures, or there are politically affiliated or otherwise exposed people in the business' senior leadership. This could take the form of board membership/composition, profit sharing agreements, funding injections or significant shareholdings. These aspects can be identified through examination of relevant interests (as defined in the *Corporations Act 2001*), corporate reporting, annual statements, solvency resolutions and registers of company members.
- Historical Practices – refers to where the business has been subject to historical proceedings, findings, assessment or reporting that have determined, or inferred, the business to be operating under FOCI. These sources could be open or closed in nature.

These indicators should be considered in the context of the proposal or evaluation, the entity's threat environment, and the entity's risk thresholds. This list is not exhaustive – entities may have indicators unique to their own operating environment and those should also be considered. There is no indicator alone that would be definitive proof of an organisation operating under FOCI.

ASIO's Due Diligence Integrity Tool (available to government personnel on GovTEAMS) provides a framework for considering some of the security risks associated with foreign collaboration.

6.1.3.2. Assess Potential FOCI Risks

Not all instances of FOCI will create unacceptable security risks but security risks should be considered as part of all procurement and contract decisions involving providers operating under FOCI.

When preparing a risk assessment of potential FOCI risks, entities should consider:

- What is the likely outcome of proceeding with the procurement?
- What are the potential consequences, or harms, associated with proceeding with the procurement?
- What is the likelihood of FOCI risks being realised?
- How could FOCI risks be realised?
- How reliable is the information used to determine FOCI risks?

- What mitigations could be implemented to minimise FOCI risk, and do those measures introduce risk in other areas of the entity, or with the public?

6.1.3.3. Treat Potential FOCI Risks

To mitigate the threat posed by vendors, entities may have to compromise on up-front costs. This may mean spending more on products and services delivered by secure and verifiable technologies and vendors. An up-front investment in a more secure product can reduce disruption and result in significant savings in the longer term.

Risk treatments should be commensurate to the identified risk. Suggested treatment outcomes are:

- Nil action – there is insufficient risk to justify an intervention in relation to the vendor and product or service offering.
- Technical controls – scalable solutions to treat the specific access and control risks. There are three categories of technical controls: technical restrictions (e.g. operation system controls); technical transparency (e.g. code audits, penetration testing, open sourcing); and data localisation requirements (e.g. isolated data silos, domestic payments, transmission constraints).
- Structural requirements – the imposition of contractual obligations on a vendor (e.g. reporting on security performance, adherence to stipulated risk management policies and processes, supply chain mapping, requirements on sub-contractors).
- Diversify vendors – the risk is managed through diversification beyond a sole source to ensure there is not a single point of failure or over-reliance upon a source jurisdiction.
- Restriction – if the risk cannot be effectively treated by other means, restrict access to the vendor in procurement process, or replace the product or service if procurement has already occurred. Restriction may occur proactively, when existing contracts expire or products due for refresh, or in response to some geopolitical event.

6.1.3.4. Monitor and Review FOCI Risks

In accordance with PSPF Requirement 0044, entities are required to regularly monitor contracts to ensure that FOCI risks do not materialise during the contact period

Entities need to ensure the procured services or resources, the businesses that supply the services or resources, and where applicable, the third-party service providers that support delivery of the services and resources, continue to provide the same level of security as originally assessed.

For example, a provider may not have been compromised during initial procurement, but that does not mean they will not become a target in the future. Further, foreign countries' laws could change with little notice, potentially presenting FOCI risks during the contract period.

Recommended Approaches

- Complete a review where elevated risks are identified.
- Establish contract conditions that require the third-party service provider or vendor to notify the entity of any changes in ownership or control.
- Consider who is best placed to undertake the review in the entity, for example the Chief Information Security Officer may undertake the review in consultation with the procurement team and provide a report to the entity's audit and risk committee or security governance committee.

See PSPF Guidelines Chapter 7—Countering Foreign Interference and Espionage.

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 your entity or its operations.

PSPF Requirement 0047 mandates that entities manage, reassess and adjust the security risks arising from contractual arrangements for the provision of goods and services over the life of a contract.

Identifying and managing jurisdictional, governance, privacy and security risks associated with the use of certain third party partners is crucial, particularly for application developers, technology systems, technology equipment manufacturers, service providers and other organisations involved in distribution channels.

Additionally, 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 PSPF Guidelines Section **Error! Reference source not found.** for detailed guidance on countering foreign i nterference and espionage.

6.2.1 Vendor Risk Management

Vendor risk management is the process of identifying, analysing, monitoring and mitigating the risks that may arise when using individual vendors.

A vendor is a third party that is part of the end of an entity's supply chain and is generally defined as the business providing whole products or services directly to end customers including to both entities and individuals, whereas a supplier is situated at the beginning of the supply chain and creates, or makes available, products, materials, or services to businesses, known as a business-to-business interaction, typically to manufacturers.

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. Fairness of the process can be improved by advising those materials an entity could or will make available to businesses considering submitting a tender, so all tenderers have equal access to explanatory documentation.

6.2.1.1. Secure-by-Design

Secure-by-Design offers entities a proactive approach to security, particularly cyber security, by building in security from the onset of, and throughout, the design and development process.

PSPF Requirement 0048 mandates that entities use secure and verifiable third-party vendors, providers, partners and associated services unless business operations require use of them, and the residual risks are managed and approved by the Chief Information Security Officer.

Where possible, entities should procure technology resources from suppliers that adopt a secure-by-design approach to ensure that they are as secure and risk-free as possible.

ASD has developed six key foundations to illustrate secure-by-design aimed at assisting technology manufactures, and entities that procure from technology resource suppliers, to adopt a secure-by-design approach, including key risks, focus, and benefit areas for each foundation.

See ASD's Secure-by-Design Foundations for detailed guidance.

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 are best conducted during the initial stages of procurement.

Some supply chain risks pose a threat to national security, especially in the domains of critical technologies. Critical technologies are those that have the potential to affect Australia's national interest including those with military or dual-use applications, such as artificial intelligence, biotechnology and quantum computing. Critical minerals are essential for high-tech devices and equipment production, such as rare earth elements. These technologies and minerals, may be subject to foreign interference, espionage, sabotage, theft, diversion, or disruption by malicious actors who seek to gain an advantage or undermine the entity's interests.

Entities should choose suppliers that have demonstrated a commitment to security and transparency for all elements of the supply chain relating to their products and services.

Entities should develop, implement and maintain a supplier relationship management policy to assist with identifying relationships with suppliers that have demonstrated a commitment to the security of their products and services. Entities should record these suppliers on an approved supplier list.

Supply chain risk management applies the security risk management process, detailed in PSPF Guidelines Section 5—Security Risk Management, to identify, assess and prioritise the risks to people, information and resources.

To manage their supply chain risks, entities should:

- identify and outline the complete supply chain, including suppliers, vendors, retails, manufacturers, distributors, and any and all sub-contractors to the above (where possible), including establishing a list of these suppliers which is maintained
- understand the relevant threats and risks against the entity's supply chain through a security risk management process (see PSPF Guidelines Section 5—Security Risk Management), and
- develop expectations with the identified suppliers and vendors in their supply chain, including agreements that stipulate that supplies notify an entity of any security risks they identify in their products or services in a timely manner, to ensure transparency and to allow entities to make adequate security risk treatments, in accordance with PSPF Requirement 0042.

See PSPF Guidelines Section 5—Security Risk Management, PSPF Release 2024 (Section 6) and ASD's Cyber Supply Chain Risk Management.

7 Countering Foreign Interference and Espionage

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

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 act with integrity at all times 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.

- 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 is an activity carried out by, or on behalf of, or in collaboration with, a foreign power that is clandestine or deceptive and is conducted for intelligence collection purposes, affecting political or governmental processes; or is otherwise detrimental to the interests of Australia; or involves a threat to any person. 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.

7.1 Recognising Foreign Interference and Espionage

PSPF Requirement 0049 mandates that entities manage the security risks associated with engaging with foreign partners.

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 Australian 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.

People who secretly work for a foreign country often hide what they're doing and it may not be obvious they are working for a foreign power. People conducting acts of foreign interference could try to create a personal connection with government employees in order to influence decisions or gain information. A foreign country may also use these methods to interfere in Australian Government business decisions or operations

Potential warning signs that dealings and relationships might become foreign interference include:

- reduced transparency where more informal ways of communicating are used for work-related matters
- a suggested or implied quid pro quo, something that is given or taken in return for something else
- attempts to hide a relationship or interaction, or

- a request, suggestion or pressure to influence others to take a particular position.

See ASIO's Due Diligence Integrity Tool (available to government personnel on GovTEAMS) for further guidance on considering the security risks associated with foreign collaboration and how to seek advice or further information.

See PSPF Guidelines Section 6.1.3 for guidance on foreign influence in procurement.

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 have been corrupted or coerced into undertaking foreign interference activities on behalf of a foreign state actor and could deploy a range of intelligence gathering techniques which include:

- taking advantage of host entity or escorting personnel that have a lack of vigilance or poor security awareness
- exploiting an individual or entity's natural desire to be a good host and not offend visiting delegations, which can lead to non-compliance of security procedures, and
- feigned ignorance or forgetfulness, such as wandering into a restricted work area, or bringing uncleared electronic devices into restricted work areas.

See PSPF Guidelines Section 24—Security Zones and Section 25.4.3—Visitor Access Control.

7.1.2 International Agreements

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.

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

See PSPF Guidelines Section 12.3—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 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

Overseas 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 overseas 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.

The exploitation of mobile devices used by travelling Government personnel is a common vector for foreign interference and espionage. Mobile devices that should be protected include, but are not limited to, corporate and personal laptops, phones, tablets and any associated removable media, such as USB drivers and SD cards. The compromise of any government personnel mobile devices could impact the ongoing operation and security of an entity's business.

To limit the risks of foreign interference and espionage during overseas travel, employees should always handle physical information appropriately, adopt good cyber hygiene practices, and only discuss classified matters in approved locations and via secure communications channels.

Recommended actions while travelling include:

- not leaving luggage that contains Australian Government information or resources unattended and avoiding checking them in unless allowed under the Minimum Protections and Handling Requirements
- protecting electronic devices by:
    - not leaving them unattended

  - not connecting them to free, public or hotel Wi-Fi
  - not using public charging points
  - not storing them in hotel safes, noting these can be accessed, and
  - handling them in accordance with the Minimum Protections and Handling Requirements, noting that hotel safes can be accessed
- avoiding taking personal devices into locations where security classified meetings or discussions are held while travelling (in accordance with the Minimum Protections and Handling Requirements for non-government mobile devices)
- preferably travelling with new or clean (burner) mobile devices
- only holding PROTECTED and above security classified conversations in approved locations (i.e. not in plans, cars, hotel rooms, conference rooms or restaurants)
- being aware of your surroundings to prevent eavesdropping or exposing security classified information or resources to unnecessary harm
- limiting information about your travel plans to those with a need-to-know, for example don't post travel plans on social media, and
- contacting your departmental security team for advice if you encounter any suspicious, ongoing, unusual or persistent interactions or have security concerns while travelling.

See PSPF Guidelines Section 9.3—Minimum Protections and Handling Requirements, Section 9.8—Security Classified Discussions, Section 17.3.2—Working Remotely Outside of Australia (International) and Section 21.4.1—Reportable Changes in Circumstances.

See ASD's Travelling With Mobile Devices | Cyber.gov.au for more information on cyber security while travelling.

Contact DFAT (security.training@dfat.gov.au) for security advice related to overseas 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, and report any suspicious, ongoing, unusual or persistent interactions to ASIO via the NITRO portal on www.nitro.asio.gov.au.

7.1.5 Protecting Personal Information

PSPF Requirement 0135 mandates that personnel do not publicise their security clearance level on social media platforms, including employment-focused platforms such as LinkedIn.

PSPF Release 2024 (Section 7.1.5) further mandates that all Australian Government personnel 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.

Government personnel who post details of clearance levels, position titles, projects and specialised systems, or personal material on social media, could make themselves a more attractive target for foreign actor interference and espionage operations. Personal information and contact lists 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.

Australian Government personnel are particularly vulnerable to approaches by malicious/foreign actors if they publicise the following information on social media profiles:

- identify as an Australian Government employee
- identify they have access to security classified information or projects, or
- mention they have a security clearance.

Entities should ensure their annual security awareness training and supporting materials are sufficient to ensure all personnel understand how to protect against this threat. Using the annual security check process mandated in PSPF Requirement 0168 is another way to ensure that personnel are complying with PSPF Requirement 0135.

ASIO's Think Before You Link campaign warns Australian Government personnel to be mindful of what personal information you choose to post online. You could be targeted for information that, if shared, could have serious consequences for Australia's security, its economy or your business.

The key take away messages to avoid making yourself a target online are by:

- not advertising your security clearance publicly online (PSPF Requirement 0135)
- not revealing details of sensitive job roles or employers publicly or to unknown contacts
- thinking about the lowest level of detail that you really need to include on your profile
- using website settings to manage the information you put out about yourself, and to control who can view your profile, and
- sharing CVs or details of specific projects only with trusted and verified contacts.

See ASIO's briefing materials for Organisations, Managers and Personnel.

See PSPF Guidelines Section 3.5—Security Awareness Training and Section 13.4.1—Social Media Applications.

7.2 Countering Foreign Inferefence and Espionage

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.

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 act with integrity at all times 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.

Appropriate due diligence is required to protect Australian 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 security classified 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. This includes making informed procurement decisions. See PSPF Guidelines Section 6.1.3—Foreign Ownership, Control or Influence in Procurement.
- Raise staff awareness—ensuring personnel understand the threat, how to protect themselves and the information and resources they have access to, are responsible for; and how to report suspicious behaviour or security concerns. See PSPF Guidelines Section 3.5—Security Awareness Training.

7.3 Insider Threat Programs

Insider threats are 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 legitimate or indirect access to an entity's people, information, resources, techniques and procedures. All APS personnel 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 or resources.

There are two main types of insiders:

- Intentional insiders – individuals who deliberately or knowingly betray the trust placed in them and use their authorisation of knowledge of an entity's information, resources or processes to cause deliberate harm to that entity.
- Unintentional insiders – individuals who inadvertently or unknowingly betray the trust placed in them, either accidentally via 'human errors' stemming from a lack of security and responsibility training, or due to negligence by failing to follow proper processes or by disregarding training and induction material.
    - Unintentional insider threats can be more difficult to anticipate due to their sporadic and unplanned nature, leaving little to no discernible pattern of recognition.

Insiders may portray different personas, such as:

- accidental insider
- negligent insider
- self-motivated insider
- recruited insider, or
- coerced insider.

See Countering the Insider Threat: A guide for Australian Government for further guidance on these personas.

There are many forms of recognised insider acts, however the most commonly recognised security-related acts are unauthorised use or disclosure of information, espionage or foreign interference, abuse of office,

and sabotage. Insider threats can cause significant harm to entities due to their knowledge of (and access to) people, information and resources.

See Countering the Insider Threat: A guide for Australian Government for further guidance on different types of insider acts and the resulting impacts.

PSPF Requirement 0051 mandates that entities that manage Baseline to Positive Vetting security clearance subjects, implement an insider threat program to manage the risk of insider threat in the entity.

This requirement does not require entities to meet the same standard imposed on entities that manage TS-PA security clearance subjects that is to implement an insider threat program that meets the TOP SECRET-Privileged Access Standard. Rather, to fulfil PSPF Requirement 0051, entities need to develop an insider threat program to understand, identify and prevent insider threat, in a manner that is tailored to their operating and risk environment.

While general guidance is provided below, entities should draw on the following guidance materials to develop their insider threat program:

- Countering the Insider Threat: A guide for Australian Government – a guide for Australian Government entities to understand, identity and prevent insider threat.
- ONI's Insider Threat Program Minimum Requirements for the PSPF (available on GovTEAMS) – recommended set of principles and guidance to assist with developing an insider threat program.
- ASIO's Managing the Insider Threat – Security Manager's Guide (available on ASIO's Outreach Portal).

7.3.1 Countering the Insider Threat

An insider threat program is designed to deter, detect and mitigate actions by insiders that represent a threat to the entity's people, information or resources. An effective insider threat program aims to protect critical resources and prevent loss of security classified information by countering unintentional and intentional incidents.

An entity's insider threat programs will need to be multifaceted and utilise processes and systems that limit, control and monitor access within the entity. The insider threat program should:

- be tailored to the entity's unique strategic objectives
- use a multidisciplinary approach which considers the entity's size, culture, quantity of resources, unique threat landscape, risk appetite and risk tolerance levels
- be included in the entity's security risk management plan and security risk assessment
- support a holistic positive security culture across the entity
- include a framework that helps identify, assess, manage and mitigate the entire range of insider threat risks, and
- be supported by the entity's senior leadership team.

The entity's insider threat program should encourage support and participation from all personnel, including senior leaders. The cultural, operational and financial benefits of the insider threat program should be communicated to the workforce to achieve and maintain support for the program.

Entities should ensure their security awareness training materials educate their personnel about insider threats and how to report actual or suspected acts of insider threat. The training should also include advice

on how the entity manages the insider threat, including confidentiality provisions and supporting mechanisms, so that personnel know that how any information they provide will be handled and protected.

The training may also include:

- awareness of the threat – individuals, special interest groups, or foreign powers or their proxies that may show interest in entity personnel or meets the SOUP criteria threshold as described below
    - Suspicious – the contact didn't seem quite right
    - Ongoing – the contact has become more regular or has evolved into a friendship or relationship
    - Unusual – the contact was odd or out of the ordinary
    - Persistent – the contact is showing noticeable commitment to engaging with you despite rejection.
- transparency and vigilance – in applying entity gift policies and knowing who you are dealing with and why, and communicating securely through approved channels in approved locations.

Recommended Appproaches

- ✔ Provide personnel with clearly defined points-of-contact for them to report actual or suspected insider threat acts, or seek advice on concerns relating to insider threat.
- ✔ Senior leaders are appointed to act as 'champions' of the entity's insider threat program.

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 protective security report, of any significant issues with implementing a PSPF Requirement or standard or decisions to vary implementation.

Where exceptional circumstances prevents or affects the entity's capability to implement or maintain a PSPF requirement, and an alternative mitigation is not available, PSPF Requirement 0052 allows the Accountable Authority to vary application of a PSPF Requirement for a limited time, consistent with the entity's risk tolerance.

The exceptional circumstances provision allows the Accountable Authority to adapt to arising circumstances that affect the entity's implementation or maintenance of a particular requirement and the exception is critical the entity meeting its objectives or functions.

Exceptional circumstances:

- are unexpected, unavoidable, outside the entity's control or circumstances where the entity could not reasonably have prevented or responded to
- have a significant or demonstratively negative effect on the entity's people, information, resources or ability to operate, and
- are not routine in nature, foreseen or enduring.

Examples of exceptional circumstances include natural disasters (e.g. fires, floods, earthquakes and severe weather events) and emergency situations (e.g. pandemics, widespread medical emergencies, terrorist attack) significant security incidents (e.g. cyber-attack), and severe supply chain disruption (e.g. loss of power supply to all entity facilities).

The decision to apply this provision requires a documented risk assessment that includes details of the proposed variation. PSPF Requirement 0053 mandates that decisions to vary implementation of a PSPF Requirement or standard due to exceptional circumstances are documented in the entity's security plan.

Recommended Approach

- Consider alternative mitigation strategies during periods of exceptional circumstances to maintain appropriate protection of the impacted PSPF requirements.

8.2 Alternative Mitigations

Deliberately disregarding implementation of a PSPF requirement or standard is a security incident. However, in recognition that implementation of a PSPF requirement or standard is not always possible, the PSPF allows entities to implement an alternative mitigation.

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.

PSPF Requirement 0054 mandates that decisions to implement an alternative mitigation measure that meets or exceeds a PSPF requirement or standard are reviewed and reported annually. In such cases, the entity reports 'risk managed' for the corresponding requirement and provides the required information as detailed in PSPF Guidelines Section 4.2.2.1—Protective Security Reporting Process.

In accordance with PSPF Requirement 0054, entities must also review the need to implement an alternative mitigation each year to determine whether this approach is still valid and or required. This review takes place in the annual consideration of the security plan and during the annual protective security report.

8.3 Business Continuity Planning

PSPF Requirement 0055 mandates that 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.

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.

A business continuity plan details the action the entity will take before, during and after unexpected events and situations arise, in order to minimise the damage and recover 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.

Entities are encouraged to draw on the existing business continuity standards and guidance when developing their business continuity plan, such as:

- ISO 22301: 2019 – Security and resilience — Business continuity management systems
- ISO 22313:2020 – Security and resilience — Business continuity management systems — Guidance on the use of ISO 22301
- ISO/TS 22318:2021 – Security and resilience — Business continuity management systems — Guidelines for supply chain continuity management
- ASD's Business Continuity in a Box (Australian Cyber Security Centre)
- Business Continuity Institute (BCI) Good Practice Guidelines

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.

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.

PSPF Requirement 0057 mandates that entities plan for managing a broad range of emergencies and integrate their planning within the business continuity plan.

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 resources. 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.

Case Study: Real life example of the value of emergency management

Rick Rescorla understood the value of business continuity and emergency management. As Morgan Stanley's Vice President of Security, he created a stringently rehearsed security awareness training and disaster plan. He ensured that all staff from the CEO down, participated in regular security drills that included test evacuations, which was no mean feat given they were located on the 44th floor of the Word Trade Centre Tower 1.

This training was put to the test on 11 September 2001 (9/11) when a plane hit Tower 1 during a terrorist attack, something that Rick had factored into the risk assessment for his organisation. Employing his security and emergency management plans and processes, Rick was able to lead 2,700 of his co-workers out of the burning building to safety. A true hero, Rick then went back into the building in a final attempt to help the final 12 Morgan Stanley workers before the building collapsed with him inside.

Read more about this story at Recognizing War Hero Who Led WTC Survivors to Safety on 9/11 | National September 11 Memorial & Museum

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 but may also require assistance to contain or remediate emergencies. See PSPF Guidelines Section 3.6 for guidance on security incidents.

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.

The NSR:

- provides whole-of-government all-hazards monitoring and reporting – this include supports decision-making before, during and after crises
- primarily focuses on domestic events but does monitor international events that may affect Australia or its interests
- works closely with the Bureau of Meteorology, Geoscience Australia and the Australian Bureau of Statistics in order to support information sharing and collaborative outcomes
- manages the National Joint Common Operating Picture (NJCOP) that provides all-hazards situational awareness and impact related information, and
- manages the National Security Hotline, which is the central point of contact for Australians to report concerns about possible signs of terrorism and foreign interference

PM&C issued the latest version of the Australian Government Crisis Management Framework (AGCMF) in September 2024. This Framework takes an all-hazards approach to crisis management, recognising the need for consistency across the Australian Government's crisis management systems in preparation for the full spectrum of hazards that may affect life, property or the natural environment.

The Framework outlines how the Australian Government prepares for, responds to and supports recovery from crises by:

- providing an overview of the Australian Government crisis management arrangements
- outlining the Australian Government's approach to crisis preparedness, including crisis preparedness arrangements and capabilities, and
- articulating the requirements for Australian Government responses spanning near-term preparedness, response, relief and early recovery by:
    - designating the lead Australian Government ministers, senior officials and agencies required to coordinate responses to identified hazards
    - outlining the roles and responsibilities of Australian Government ministers and senior officials
    - detailing the approach to coordination for extreme to catastrophic crises.

Part Three

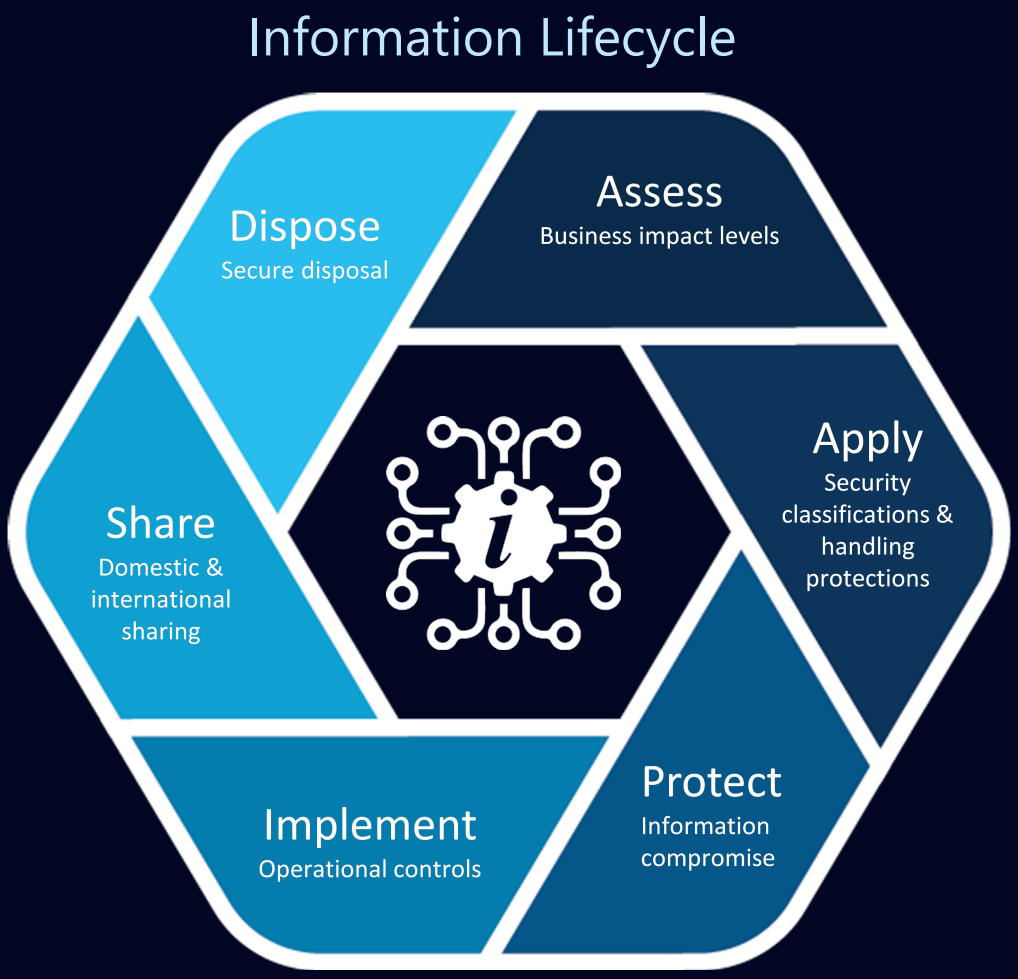
Information

Classifications and Caveats

Information Holdings

Information Disposal

Information Sharing



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 comprises 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 resources that process, store or communicate 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.

- Confidentiality – limits access to authorised persons for approved purposes (who can access the information and why).
- Integrity – assures that information is only being created, amended or deleted by the intended authorised means and is correct and valid.
- Availability – ensures authorised persons have access to information when and as needed.

The National Archives of Australia Australian Government Information Management Standard notes that information is a valuable asset. It contributes to good government through supporting efficient business, informing decision-making, demonstrating government accountability and transparency, mitigating risks, adding economic value and protecting rights and entitlements.

9.1 Originator

The originator is the entity that initially generated the information, or first received the unmarked information (i.e. where an Australian Government or third-party approved security classification has not been applied) from outside the Australian Government, and which has 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.

To ensure continuity, the entity may set the originator as the person, role, delegation or section within the entity that is best placed to be responsible for controlling the information.

If the entity, or functions of the entity, are abolished or merged, for example as part of a Machinery of Government change, then the entity assuming the former entity's responsibilities, is now considered the originator. These changes also present an opportunity to re-assess the security classification of information.

Assessing the security classification of information when it is first created or received from outside the Australian Government helps to protect the information. The originator can also set a specific date or event for automatic declassification. See PSPF Guidelines Section 9.1.1—Sanitisation, Reclassification or Declassification.

Case study: Originator Impacted by Machinery of Government Change

An officer working in Entity X is the originator of a PROTECTED document. The section in which the officer works is scheduled to transfer to Entity Y on 22 December 2023, however, the officer has transferred to another role in the entity, and will therefore not be transferring to Entity Y. In this case, the section in Entity Y that is assuming the responsibility for the incoming functions from Entity X, becomes the originator for the PROTECTED document in question. A senior officer in Entity Y assigns responsibility for the document (or multiple incoming documents) either to a person, role or section within Entity Y to be the originator of the information from the date of transfer. Entity X documents the transfer to Entity Y, and Entity Y documents the decision to reassign the responsibility.

The originator is responsible for applying the relevant marking or security classification. To do this they must assess the Business Impact Level (BIL) based on the likely damage if the information's confidentiality was compromised. See PSPF Guidelines Section 9.2—Security Classifications for Business Impact Level Tool.

9.1.1 Sanitisation, Reclassification or Declassification

PSPF Requirement 0058 mandates that 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.

Information may require modification to allow its wider distribution and potential use. Only the originating entity can change the security classification applied to its information. If the application of a security classification is considered inappropriate, the original classification decision can be queried with the originator.

Consistent with PSPF Requirement 0058, information that has been reclassified or declassified must be clearly identified using an applicable marking or security classification to reflect the new assessment of the Business Impact Level.

Examples are provided below for reclassifying, sanitising or declassifying information, however entities can determine the approach that best suits their business needs and operating environment.

- Sanitisation – the process to remove, conceal or change information by editing, redacting or altering information to reduce its security classification to protect intelligence, sources, methods, capabilities, analytical procedures or privileged information.
    - Sanitising electronic documents in word processing software such as MS Word:
        - Find and replace/remove all the text to be redacted in the original file and save it as a new file using the original file name, adding sanitised version and the date to the file name. E.g. Title – sanitised version – 31 August 2024. Save the document as a PDF before sharing it.

        I, [content redacted] of [content redacted] agree to .....

        - Do not use black shapes over the text being redacted or make the text another colour (e.g. white) to obscure from view, otherwise, the redacted text will only be hidden from view but not removed from the document and the text can still be accessed by copying and pasting and is searchable. See the Federal Court of Australia's Guide to Redacting Documents in Electronic Form for advice.
        - Remember to also remove the metadata from the document by using the 'inspect document function'.
    - Sanitising physical documents or information:
        - Photocopy the original source document and then obscure the relevant content by means of wide black pen or opaque tape, before photocopying the document and before sharing. It is important to ensure the originator retains a copy.
        - This approach requires precision to ensure all the sanitised information is fully obscured and the exact length of the content or individual words are unrecognisable or not easily guessed.

        I, [redacted] of [redacted] agree to .....

- Reclassification – an administrative decision by the originator to change the security classification of information based on a reassessment of the potential impacts of its compromise. Reclassification may raise or lower the security classification of information.
    - The recommended approach is to strike out the original classification and add a new classification, then type (or write) the name, role, delegation or section of the originator, the date the reclassification was approved, and the document management system reference of originator's approval.

~~TOP SECRET~~ SECRET
Reclassification approved by Joe Smith, Director of Special Classification Projects on 31 August 2024, ADD2024/1234567.

- Declassification – an administrative decision by the originator to reduce the security classification of information to OFFICIAL (an unclassified state) when it no longer requires security classification handling protections.

~~OFFICIAL: Sensitive~~ OFFICIAL

Recommended Approaches

- Develop an entity procedure for noting when the originator has approved the reclassification or declassification of information.
- Establish procedures so that information is automatically declassified if the originator sets a specific date or event for declassification based on an assessment of the period in which the information might cause damage, otherwise when the open access period ceases under the *Archives Act 1983*.
- Establish procedures to encourage regular reviews of classified information for continuing sensitivity (i.e. if the compromise of the information would still cause damage) using the impact-based classification assessment.
    - For example, these reviews could be done after a project is completed or when a file is withdrawn from (or returned to) use. Information is declassified or reclassified to a lower classification when a reassessment of its Business Impact Level indicates it no longer meets the original Business Impact Level to which its classification applies.

See the National Archives of Australia website for guidance on open access periods.

9.1.2 Official Information Designated for Public Release

Information assessed as OFFICIAL may be authorised for public release, access or circulation (for example, entity publications or website content) by the originator, within the limits of authority conferred on them by the entity.

If designated for public release, then either:

- omit the optional OFFICIAL protective marking from the information, or
- mark the information to reflect that it is intended and suitable for public release or publication, either with or without the non-mandatory OFFICIAL protective marking.

While not mandatory, entities may elect to adopt the Australian Government Record Keeping Metadata Standard 'Rights Type Scheme' term, 'Authorised Public Access'. This term can be applied with or without the non-mandatory OFFICIAL protective marking.

Information intended for public release or publication could have sensitivity requirements or restrictions prior to being released. For example, Budget papers. In this case, the point at which the information will be publicly available is recommended to be marked.

All personal information held—even if it is publicly available—is to be handled in accordance with the Australian Privacy Principles (APPs) in the *Privacy Act 1998*.

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.

It is important that the management of information enables entities to meet business, government and community needs and expectations—this involves balancing the need to protect information with the need to ensure appropriate access.

Appropriately limiting the quantity, scope or timeframe of security classified information:

- promotes an open and transparent democratic government
- provides for accountability in government policies and practices that may be subject to inappropriate or over-classification
- allows external oversight of government operations and programs, and
- promotes efficiency and economy in managing information across government.

It is not consistent with the PSPF to apply a security classification to information in order to:

- restrain competition
- hide violations of law, inefficiency, or administrative error to prevent embarrassment to an individual, organisation or entity, or
- prevent or delay the release of information that does not need protection.

A security classification (OFFICIAL: Sensitive, PROTECTED, SECRET and TOP SECRET) is only applied to information (or resources that process, store or communicate security classified information) if it requires protection because the impact of compromise of the information or asset would be low to medium, or above.

The requirements in this policy do not displace obligations imposed on entities through other policies, legislation or regulations, or by any other means.

9.2.1 Assess Security Classification

PSPF Requirement 0059 mandates that the originator assesses the value, importance or sensitivity of official information (intended for use as an official record) by considering the potential damage to the government, the national interest, organisations or individuals that would arise if the information's confidentiality was compromised, using the levels described in Table 17.

Information compromise includes, but is not limited to, loss, misuse, interference, unauthorised access, unauthorised modification, or unauthorised disclosure.

Table 17: 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.

In accordance with PSPF Requirement 0060, the security classification of information must be set at the lowest reasonable level, as over-classification of information can result in:

- access to official information being unnecessarily limited or delayed
- onerous administration and procedural overheads that add to costs, or
- classifications being devalued or ignored by personnel and receiving parties.

The person responsible for generating or preparing information on behalf of an entity (or for actioning information produced outside the Australian Government) assesses whether the information needs to be security classified. Only the originator can change the security classification applied to its information. If the application of a classification is considered inappropriate, the original classification decision can be queried with the originator.

9.2.2 Business Impact Level

The more valuable, important or sensitive the official information, the greater the impact on government business that would result from its compromise. By assessing the 'Business Impact Level' if confidentiality of the information is compromised, the originator can determine whether information requires a security classification or requires a routine level of protection.

The Business Impact Levels tool (see Table 18) provides examples of potential damage from compromise of information's confidentiality. The tool assists in the consistent classification of information and the assessment of impacts on government business. Entities may develop their own sub-impact categories.

The potential damage from compromise of information's confidentiality determines the classification of that information. A simple flow diagram is provided in Figure 9 to help assess whether information is security classified, based on the potential damage from compromise of the information's confidentiality.

The Business Impact Levels tool can also be used for secondary assessments of the potential damage from compromise of the availability or integrity of information. While assessing the Business Impact Level of compromise of the information's availability or integrity does not affect whether the information is security classified information, it may indicate that additional security measures could be warranted, such as cyber, personnel or physical controls.

Table 18: Business Impact Level Tool - Assessing damage to the National Interest, Government, Organisations or Individuals

Sub-Impact Category	Security Classified Information (Mandatory)				Non-mandatory
	TOP SECRET	SECRET	PROTECTED	OFFICIAL: Sensitive	OFFICIAL
	5 Catastrophic Business Impact The most valuable, important and sensitive information. Compromise of TOP SECRET information would be expected to cause exceptionally grave damage to the national interest, organisations or individuals.	**4 Extreme Business Impact** Very valuable, important and sensitive information. Compromise of SECRET information would be expected to cause serious damage to the national interest, organisations or individuals.	**3 High Business Impact** Valuable, important and sensitive information. Compromise of PROTECTED information would be expected to cause damage to the national interest, organisations or individuals.	**2 Low to Medium Business Impact** OFFICIAL information that due to its sensitive nature requires limited dissemination. Compromise of OFFICIAL: Sensitive information would be expected to cause limited damage to an individual, organisation or government.	**1 Low Business Impact** The majority of official information created or processed by the public sector. Includes routine business operations and services. OFFICIAL is not a security classification and compromise of OFFICIAL information would not result in damage to individuals, organisations or government.
Potential impact on individuals from compromise of the information					
Dignity or safety of an individual (or those associated with the individual)	Exceptionally grave damage is: • widespread loss of life, or • discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to directly lead to the death of a large number of people.	Serious damage is discrimination, mistreatment, humiliation or undermining people's dignity or safety that could reasonably be expected to directly threaten or lead to the loss of life of an individual or small group.	Damage to an individual is discrimination, mistreatment, humiliation or undermining of an individual's dignity or safety that leads to potentially significant harm or potentially life-threatening injury.	Limited damage to an individual is: • potential harm, for example injuries that are not serious or life threatening, or • discrimination, mistreatment, humiliation or undermining an individual's dignity or safety that is not life threatening.	Information from routine business operations and services. Includes personal information as defined in the Privacy Act .[Note i] This may include information (or an opinion) about an identifiable individual (e.g. members of the public, staff etc.) but would not include information defined as sensitive information under the Privacy Act.
Potential impact on organisations from compromise of the information					
Entity operations, capability and service delivery	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.	Serious damage to entity operations is: • a severe degradation in, or loss of, organisational capability to an extent and duration that the entity cannot perform any of its functions • directly threatening the internal stability of Australia.	Damage to entity operations is: • a degradation in, or loss of, organisational capability to an extent and duration that the entity cannot perform one or more of its primary functions • major loss of confidence in government.	Limited damage to entity operations is: • a degradation in organisational capability to an extent and duration that, while the entity can perform its primary functions, the effectiveness of the functions is noticeably reduced • minor loss of confidence in government.	Information from routine business operations and services.
Entity assets and finances, e.g. operating budget	Not applicable. Impacts on an entity or organisation due to compromise of information are assessed as to the level of impact to the national interest.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Damage is: • substantial financial loss to an entity • $100 million to $10 billion damage to entity assets.	Limited damage to entity assets or annual operating budget is equivalent to $10 million to $100 million.	Information compromise would result in insignificant impact to the entity assets or annual operating budget.
Legal compliance, e.g. information compromise would cause non-compliance with legislation [Note ii] commercial confidentiality or legal professional privilege	Not applicable. Impacts on an entity or organisation due to the compromise of information are assessed as to the level of impact to the national interest.	Not applicable. Impacts on an entity or organisation at this scale are considered a matter of national interest.	Damage is failure of statutory duty or breaches of information disclosure limitations under legislation resulting in two or more years' imprisonment.	Limited damage is: • issues of legal professional privilege for communications between legal practitioners and their clients • contract or agreement non-compliance • failure of statutory duty • breaches of information disclosure limitations under legislation resulting in less than two years' imprisonment.	Information compromise would not result in legal and compliance issues.
Aggregated data [Note iii]	A significant aggregated holding of sensitive or classified information that, if compromised, would cause exceptionally grave damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive or classified information that, if compromised, would cause serious damage to the national interest, organisations or individuals.	A significant aggregated holding of sensitive information that, if compromised, would cause damage to the national interest, organisations or individuals.	A significant aggregated holding of information that, if compromised, would cause limited damage to the national interest, organisations or individuals.	An aggregation of routine business information.
Potential impact on government or the national interest from compromise of the information					
Policies and legislation	Exceptionally grave damage to the national interest is the collapse of internal political stability of Australia or friendly countries.	Serious damage to the national interest is a severe degradation in development or operation of multiple major policies to an extent and duration that the policies can no longer be delivered.	Damage to the national interest is: • impeding the development or operation of major policies • revealing deliberations or decisions of Cabinet, or matters submitted, or proposed to be submitted, to Cabinet [Note iv] (not otherwise captured by higher level business impacts).	Limited damage to government is impeding the development or operation of policies.	Information compromise from routine business operations and services. For example, this may include information in a draft format (not otherwise captured by higher business impact level).

Australian economy	Exceptionally grave damage to the national interest is the collapse of the Australian economy.	Serious damage to the national interest is: • undermining the financial viability of an Australian industry sector (multiple major organisations in the same sector) • long-term damage to the Australian economy to an estimated total in excess of $20 billion.	Damage to the national interest is: • undermining the financial viability of a major Australian-based or owned organisation or company • disadvantaging a number of major Australian organisations or companies • short-term material impact on national finances or economy.	Limited damage to government is: • undermining the financial viability of one or more individuals, minor Australian-based or owned organisations or companies • disadvantaging a major Australian organisation or company.	Information from routine business operations and services.
National infrastructure	Exceptionally grave damage to the national interest is the collapse of all significant national infrastructure.	Serious damage to the national interest is shutting down or substantially disrupting significant national infrastructure.	Damage to the national interest is damaging or disrupting significant state or territory infrastructure.	Limited damage to government is damaging or disrupting state or territory infrastructure.	Information from routine business operations and services.
International relations	Exceptionally grave damage to the national interest is directly provoking international conflict or causing exceptionally grave damage to relations with friendly countries.	Serious damage to the national interest is: • severely disadvantaging Australia in major international negotiations or strategy • directly threatening internal stability of friendly countries, leading to widespread instability • raising international tension or severely disrupting diplomatic relations resulting in formal protest or sanction.	Damage to the national interest is: • short-term damage or disruption to diplomatic relations • disadvantaging Australia in international negotiations or strategy.	Limited damage to government is minor and incidental damage or disruption to diplomatic relations.	Information from routine business operations and diplomatic activities.
Crime prevention, defence or intelligence operations	Exceptionally grave damage to the national interest is significantly affecting the operational effectiveness, security or intelligence operations of Australian or allied forces.	Serious damage to the national interest is major long-term impairment to the ability to investigate or prosecute serious organised crime [Note v] affecting the operational effectiveness, security or intelligence capability of Australian or allied forces.	Damage to the national interest is: • impeding the detection, investigation, prosecution of, or facilitating the commission of an offence with two or more years imprisonment • affecting the non-operational effectiveness of Australian or allied forces that could result in risk to life.	Limited damage to government is: • impeding the detection, investigation, prosecution of, or facilitating the commission of low-level crime • affecting the non-operational effectiveness of Australian or allied forces without causing risk to life.	Information from routine business operations and services.

Table Notes

[i] Section 6 of the *Privacy Act 1988* provides definitions of 'personal information' and 'sensitive information':

'*personal information* means information or an opinion about an identified individual, or an individual who is reasonably identifiable:

- whether the information or opinion is true or not; and
- whether the information or opinion is recorded in a material form or not.'

'*sensitive information* means:

- information or an opinion about an individual's:
  - racial or ethnic origin; or
  - political opinions; or
  - membership of a political association; or
  - religious beliefs or affiliations; or
  - philosophical beliefs; or
  - membership of a professional or trade association; or
  - membership of a trade union; or
  - sexual orientation or practices; or
  - criminal record;

  (that is also personal information); or
- health information about an individual; or
- genetic information about an individual that is not otherwise health information; or
- biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
- biometric templates.'

Where compromise of personal information, especially sensitive information under the Privacy Act would lead to damage, serious damage or exceptionally grave damage to individuals, this information warrants classification.

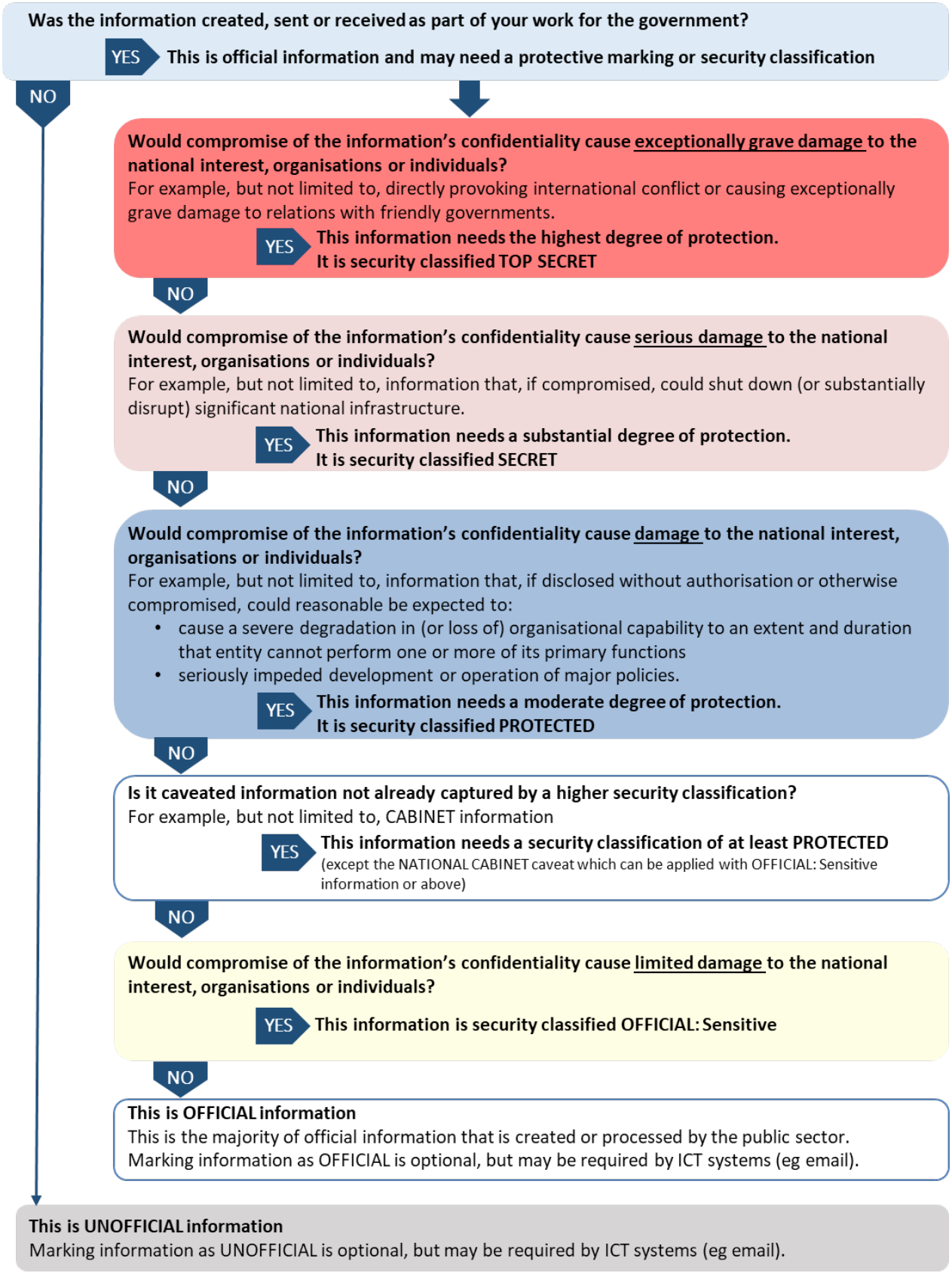
[ii] In its report Secrecy Laws and Open Government in Australia the Australian Law Reform Commission identified 506 secrecy provisions in 176 pieces of legislation, including 358 distinct criminal offences. Examples of legislation including secrecy provisions include: *Social Security Act 1991* and *Social Security (Administration) Act 1999, Taxation Administration Act 1953, Census and Statistics Act 1905*, and, more generally, the *Criminal Code Act 1995*.

[iii] A compilation of information may be assessed as requiring a higher security classification where the compilation is significantly more valuable than its individual components. This is because the collated information reveals new and more sensitive information or intelligence than would be apparent from the main source records and would cause greater damage than individual documents. When viewed separately, the components of the information compilation retain their individual classifications. See Annex H for guidance on assessing aggregated and integrated data.

[iv] This includes official records of Cabinet, Cabinet business lists, minutes, submissions, memoranda or matters without submission, and any other information that has been submitted or proposed to be submitted to Cabinet.

[v] Serious organised crime as defined in the Convention Against Transnational Organised Crime.

Figure 9: Security Classification Flow Chart



9.2.3 Mark Security Classification

Applying a security classification indicates that the information requires protection, and dictates the level of protection required. Security classifications help control and prevent compromise of information as they are an easily recognisable way for information users (visually) and systems (such as an entity's email gateway) to identify the level of protection the information requires.

The OFFICIAL marker may be used to identify information that is an Australian Government record that is not security classified. Similarly, the UNOFFICIAL marker may be used to identify information generated for personal or non-work related purposes. Use of these markers is not mandatory.

9.2.3.1. Text-based Markings

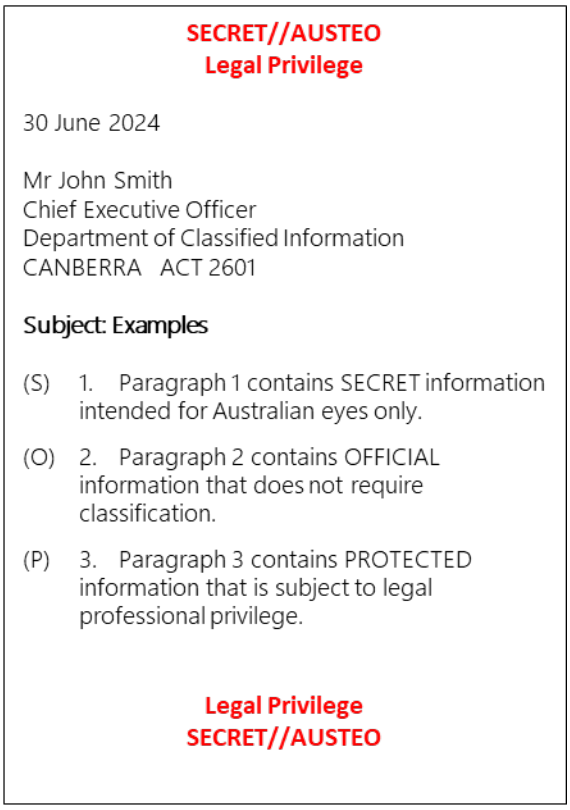
PSPF Requirement 0061 mandates that security classified information is clearly marked with the applicable security classification, and when relevant, security caveat, by using text-based markings, unless impractical for operational reasons. See PSPF Guidelines Section 9.7—Recordkeeping Metadata Standard for information on marking information on systems that store, process or communicate security classified information.

PSPF Requirement 0061 indicates that text-based security classifications are the preferred method to identify security classified information. Figure 10 provides an example of applying security classifications to physical information.

Figure 10: Marking physical (printed) information

In this example:

- Paragraph 1 contains the most valuable, important and sensitive information in the document. The information in this paragraph dictates the document's overall classification.
- Compromise of the information in paragraph 1 could be expected to cause serious damage to the national interest, organisations or individuals. The information in paragraph 1 is classified as SECRET. This means the document's overall classification is also SECRET.
- Additionally, the information in paragraph 1 can only be accessed by Australian citizens and the AUSTEO caveat has been applied. See Security Caveats.
- Paragraph 3 contains information that is subject to legal privilege. See Information Management Markers.
- To meet the classification requirements, the SECRET marking is conspicuously applied to the top and bottom of the page. An AUSTEO caveat marking is also applied. The double forward slash helps to clearly differentiate each marking. As this entity uses the optional information management markers, the legal privilege marking is also applied.
- The entity has also used the optional paragraph grading indicators to mark each paragraph separately. See Minimum Protections and Handling Requirements.



See PSPF Guidelines 9.6—Email Protective Marking Standard for marking emails and Recordkeeping Metadata Standard.

9.2.3.2. Colour-based Markings

If text-based markings cannot be used (e.g. on certain media or assets), colour-based markings must be used.

Colour-based markings use the RGB model, which refers to Red (R), Green (G) and Blue (B) colours that can be combined in various proportions to obtain any colour in the visible spectrum. Alternatively the CMYK colour model may be used.

Table 19 specifies the recommended RGB colour-based marking that applies to each security classification. There are no specific RGB colours for OFFICIAL: Sensitive and OFFICIAL information, although a Yellow colour is recommended for OFFICIAL: Sensitive.

Table 19: RGB and CMYK cell colour for colour-based markings

Security classification	Colour-based marking	RGB cell colour	CMYK cell colour
OFFICIAL: Sensitive	Yellow	R 255, G 242, B 204	C 0%, M 5%, Y 20%, K 0%
PROTECTED	Blue	R 79, G 129, B 189	C 58%, M 32%, Y 0%, K 26%
SECRET	Pink/Salmon	R 229, G 184, B 183	C 0%, M 20%, Y 20%, K 10%
TOP SECRET	Red	R 255, G 0, B 0	C 0%, M 100%, Y 100%, K 0%

If both text-based and colour-based markings cannot be used (e.g. for verbal information), entities must use a scheme to identify security classified information. The scheme must be documented and entities must train personnel appropriately on how to use the scheme.

For example, a scheme could include an entity policy for meetings that may include discussion of security classified information, in which participants identify at the commencement of the meeting the level of security classified information to be discussed.

Other markings, are not recognised by this policy, for example entity-specific markings. A standard set of markings ensures common understanding, consistency and interoperability across systems and government entities. Other markings may confuse users about appropriate handling protections.

Once marked, security classified information must be protected and handle in accordance with the Minimum Protections and Handling Requirements. See PSPF Guidelines 9.3—Minimum Protections and Handling Requirements for detailed guidance.

9.2.3.3. Documents Covering Multiple Security Classifications

In cases where a principal document has multiple attachments, annexes or appendices each with differing security classifications, the document's front cover is to represent the highest security classification.

Options for a document covering 2 appendices of differing security clearance include:

- Option 1: mark the covering (or principal) document with the appropriate marking or security classification and note it covers annexes or appendices of a higher classification.

  Principal document marking: PROTECTED covering SECRET

  Annex 1 marking: PROTECTED

  Annex 2 marking: SECRET

  - This approach allows the principal document and Annex 1 to be handled as PROTECTED in accordance with PSPF Requirement 0060 to set the security classification at the lowest reasonable level, but ensures Annex 2 is handled as SECRET.
  - This means the principal document and Annex 1 could be stored on a PROTECTED network and Annex 2 on a SECRET network.
  - Option 1 is particularly effective for printed (hard copy) documents or meeting papers with multiple attachments of differing security classifications.

- Option 2: mark the covering (or principal) document with the highest security classification present in all annexes or appendices.

  Principal document marking: SECRET

  Annex 1 marking: SECRET

  Annex 2 marking: SECRET

- This is a more conservative approach but does impose higher protections and handling requirements on all the documents involved as both the principal document and all annexes must be stored on a SECRET network.

9.3 Minimum Protections and Handling Requirements

PSPF Requirement 0062 mandates that the minimum protections and handling requirements are applied to protect OFFICIAL and security classified information. These protections and handling requirements establish the key operational controls for accessing, using, storing, carrying, transmitting, disposing, communicating or travelling with OFFICIAL and security classified information in physical formats and on government-issued mobile devices and non-government issued mobile devices.

Table 20 describes the types of mobile devices covered by the minimum protections and handlings requirements, including the two types of non-government mobile devices–authorised non-government devices and all other devices.

Table 20: Mobile Device Types

Item	Description
Government-issued mobile device	Mobile or portable computing communications device that is owned and issued by an Australia Government entity to access government systems and information, configured, encrypted and managed to ASD standards and guidance (as detailed in the ISM), and is approved by the relevant authority to process, store or communicate entity information of a specified classification. • Includes: mobile phones, handheld computers, tablets, laptops and digital assistants. • If these requirements are met, then a government-issued mobile device is considered in a 'secured state'. • This also includes Australian Government-issued mobile devices that for operational reasons are connected to isolated networks, for example standalone or air gapped devices.
Non-government mobile device	**Authorised non-government device** Mobile or portable computing communications devices owned or issued by a non-government source (for example commercial organisation, non-government organisation, industry-issued or privately owned) that is configured, encrypted and managed in accordance with ASD standards and guidance, and the residual risk is accepted by the Australian Government entity system risk owner to access, process, store or communicate OFFICIAL, OFFICIAL: Sensitive, PROTECTED Australian Government information or data. • Includes: mobile phones, handheld computers, tablets, laptops and digital assistants. • Non-government devices must not access, process, store or communicate SECRET or TOP SECRET information or data. • 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, then the device is considered in an 'unsecured state'.
Non-government mobile device	**All other mobile devices** Devices that are not owned, issued or authorised by the entity. See ISM for additional controls. • 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. • 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 required in a Zone 3, then use is subject to risk assessment and approval by the CSO or CISO. **Medical devices**

Item	Description
	The all other mobile devices category 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. 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 and Zone 3 areas where TOP SECRET or SECRET information or resources are present. Medical devices can be used in a: • Security Zone 3, except where TOP SECRET or SECRET information/devices are present. In this situation, medical devices can be used provided a risk assessment is undertaken and approved by the CSO/CISO of the entity, and appropriate controls are put in place. • Security Zone 4, provided a risk assessment is undertaken and approved by the CSO/CISO of the entity, and appropriate controls are put in place. • Security Zone 5, provided a risk assessment is undertaken and approved by ASD, and appropriate controls are put in place. These arrangements ensure PSPF Release 2024 requirements remain aligned with existing ISM controls which are mandated under ASIO's *Technical Note 1/15 – Physical Security Zones*. The ASIO Tech Note, established since 2016, is mandated under PSPF Requirement 0194. It was also mandated under the previous PSPF. • ASD's ISM prohibits unauthorised radio frequency and infrared devices from being used in Zone 4 and Zone 5 areas (ISM control number 0225). • ASD's Risk Management of Enterprise Mobility (Including Bring Your Own Device) requires a business case for use of personally owned devices. The Department of Health and Aged Care's Therapeutic Goods Administration also provides guidance for manufacturers and sponsors on the cyber security of medical devices that include software or electronic components. This guidance aligns with the approach in the PSPF and ISM by requiring medical devices to include 15 'Essential Principles' which are set out in Schedule 1 of the *Therapeutic Goods (Medical Devices) Regulations 2002*, which relate to the safety and performance characteristics of medical devices. For a medical device to be included on the Australian Register of Therapeutic Goods, the manufacturer must demonstrate compliance with the Essential Principles. The Essential Principles require that a manufacturer minimise the risks associated with the design, long-term safety and use of the device – this implicitly includes minimisation of cyber security risk. Six general Essential Principles are relevant to all medical devices, and a further nine Essential Principles about design and construction apply to medical devices on a case-by-case basis, depending on the technology used within the device. The relevant guidelines are below: • Complying with medical device cyber security requirements • Medical device cyber security information for users • Medical device cyber security guidance for industry

See ISM for controls for private mobile devices, virtual desktop solutions and non-mobile desktop equipment and servers.

Recommended Approaches

- Ensure the use or presence of privately-owned mobile devices do not present an unacceptable security risk.
- Develop entity-specific protections for security classified information where a higher level of protection is required to meet business needs or the entity's security risk environment.
- Develop procedures for assessing the risks of medical devices to support staff working in Zones 4 and 5.

9.3.1 Store Security Classified Information

Security classified information is considered 'unattended' when it is not under the immediate control of in the physical presence of the person responsible for it (or their suitable delegate). PSPF Release 2024 (Section 9.3) requires entities to store information and devices securely when unattended in the appropriate security container for the approved zone to protect from compromise.

See PSPF Guidelines Section 25.2—Security Containers, Cabinets and Rooms for details of lockable containers.

Mobile devices must be stored in a secured state. A mobile device is considered in a 'secured state' if it is configured, encrypted and managed in accordance with ASD standards and guidance, and encryption is active when the device is not in use. A mobile device that doesn't meet a 'secured state' is considered in an 'unsecured state'.

See ISM's Guidelines for Cryptography.

The National Archives of Australia Australian Government Information Management Standard requires that entities store information securely and preserve it in a usable condition for as long as required for business needs and community access. In accordance with the Information Management Standard, a secure and suitable storage environment is one that prevents unauthorised access, duplication, alteration, removal and destruction.

Ways to minimise duplication or alteration of information include:

- reproducing security classified information only when necessary, and
- immediately destroying spare or spoilt copies (such destruction is defined as 'normal administrative practice' in the *Archives Act 1983* and does not need specific permission from the National Archives of Australia).

The minimum protections and handling requirements detailed in PSPF Release 2024 also make allowances for security classified information to be stored in exceptional circumstances. Where required but not specified, the Accountable Authority, CSO or CISO can approve alternative arrangements.

See PSPF Guidelines Section 8.1—Exceptional Circumstances and Section 9.3—Minimum Protections and Handling Requirements.

9.3.1.1. Clear Desk and Locking Devices

Establishing a clear desk policy and screen locking procedures are an additional way to protect information when unattended. These procedures promote awareness of the requirements to protect information from compromise and assist entity personnel to secure all files, documents (electronic as well as paper), security classified material (including portable and attractive items, for example iPads, mobile phones, memory sticks, portable hard drives) and other official information in their custody.

In addition to applying the minimum protections and handling requirements for unattended security classified information, personnel should apply the following procedures whenever a desk, workspace or office is left unattended or at the end of the day:

- Security classified information is stored appropriately (or for brief absences, passed to a colleague with the appropriate security clearance and briefings for safe keeping until the responsible person returns to claim the information)
- Mobile devices are locked when not in use or left unattended using Ctrl + Alt + Del, or (Windows + L) for PC, and (Command + Control + Q) for Mac, and requires the user to authenticate to unlock the session
- Mobile devices are shut down at the end of the work day

- Portable and valuable items are secured, including electronic media containing security classified information
- Keys to classified storage devices are secured (particularly when visitors or uncleared personnel are present), and
- Keys are not left in doors or drawers at the end of the day or for extended periods of time.

See ISM's Guidelines for System Hardening for applying session and screen locking procedures.

9.3.2 Carry Security Classified Information

In accordance with PSPF Requirement 0062 the minimum protections and handling requirements for carrying each level of security classified information must be applied, including for carrying outside entity facilities and between entity facilities.

It is important to implement effective protections when carrying security classified information from one location to use in another location, including to attend meetings inside entity facilities, outside and between entity facilities. Higher levels of protection are required if security classified information is carried through a less secure zone (e.g. carrying SECRET material through a Zone 1 or carrying TOP SECRET information through a Zone 1 or Zone 2) or outside the entity in public spaces.

ASIO-T4 and the Security Construction and Equipment Committee (SCEC) provide advice on security equipment for protecting classified information while carrying it. This includes advice on SCEC-endorsed tamper evident seals and packaging, as well as guidance on selecting briefcases suitable for the carriage of security classified information. The advice is available on the Protective Security Policy GovTEAMS community.

See PSPF Guidelines Section 9.3.3—Transfer and Transmit Security Classified Information for guidance on transferring information to another person or entity.

Recommended Approach

- ✔ Mobile devices are not stored in locations where meetings or discussions of a higher classification are held unless the device is protected by a visual and audio suppression container.

9.3.3 Transfer and Transmit Security Classified Information

In accordance with PSPF Requirement 0062 the minimum protections and handling requirements for transferring and transmitting each level of security classified information must be applied by a means that deter and detect compromise.

To ensure security classified information is only transferred or transmitted to people with a need-to-know, entities are encouraged to identify information recipients by:

- by a specific position, appointment or named individual
- where physical information is being transferred:
  - a full location address (e.g. not a post office box for physical delivery, as this may be unattended)
  - an alternative individual or appointment where relevant (e.g. for TOP SECRET information).
- where information is being electronically transmitted, an email address exclusive to those individuals with a need-to-know (e.g. not a mailbox with unrestricted access).

Devices that are able to store and communicate information, such as laptops, notebooks, tablets, smart mobile phones, personal digital assistants and USBs, can be used to both transfer and transmit information. Ways to deter and detect information compromise and unauthorised access when devices are used include password protection, encrypting information at rest and remote wiping capabilities.

Where devices cannot be protected by these means, apply the protections used for physical information.

Where a device is being used to transfer security classified information to another entity—i.e. the device will be retained by the receiving entity—it may be appropriate for entities to consider additional controls such as receipts.

9.3.3.1. Transfer Security Classified Information

Transfer means to move security classified information from one place (or person) to another.

Examples of transferring information include:

- handing information to a person within an office environment (i.e. within entity facilities)
- sending information through the entity's internal mail to a person who works in the same building
- sending information through the entity's internal mail to a person who works in a different building
- handing or sending information to a person in another entity, or
- giving a person a secure approved USB or other storage device that holds the information.

The security measures required to protect security classified information and caveated information and material during physical transfer depend on the security classification level of the information, where the information is going from and to, and the transfer method used. Entities are required to adopt security measures when transferring physical security classified information to:

- obscure that the information is security classified, and
- deter and detect unauthorised access to the information.

The PSPF Minimum Protections and Handling Requirements establish the minimum protections to transfer each level of security classified information.

Where transfer is between physical locations:

- use a tamper-evident double barrier to protect security classified information, the most common method to achieve this is 'double-enveloping', or
- use a secure transfer method, such as entity safe hand or safe hand by an endorsed courier.

Where transfer is outside of Australia, special care is necessary and in some cases is not permitted:

- consider country-specific advice
- check with DFAT about the most appropriate method to transfer security classified information outside Australia (if not detailed in the minimum protections and handling requirements), and
- establish entity procedures if overseas transfers form a routine part of their business.

The PSPF does not impose requirements for the transfer of OFFICIAL information (as opposed to OFFICIAL: Sensitive information), however entities are recommended to ensure that OFFICIAL information is transferred by means which deter and detect compromise.

Table 21: Methods of Transfer

Method	Description
Double Enveloping	'Double enveloping' consists of: • Inner envelope – a tamper evident inner barrier to detect unauthorised access. o The inner envelope can consist of an envelope or pouch sealed with a SCEC-approved tamper evident seal so that any tampering is detected, or a SCEC-approved single use envelope. o The inner envelope is marked conspicuously with the security classifications (e.g. at the top and bottom of the front and back of the envelope).

Method	Description
	• Outer envelope – an outer barrier to obscure the information's security classification and deter unauthorised access. o The outer envelope is some form of sealed opaque covering. It could be a regular mail envelope, a SCEC-approved single-use outer envelope, security briefcase, satchel, pouch or transit bag. o The outer envelope may display information identifying the recipient and any receipt or reference numbers, if required. o The outer envelope should not be marked in a way that indicates the information in the inner envelope is security classified information.
Safe Hand	Safe hand means information is dispatched to the addressee in the care of an authorised person or succession of authorised people who are responsible for its carriage and safekeeping. An authorised person can be a responsible officer who removes the information from the entity facility, or an endorsed courier. • Sending information via safe hand establishes an audit trail that provides confirmation that the addressee received the information and helps to ensure the item is transferred in an authorised and secure facility or vehicle. To deter and detect any information tampering, at each handover, a receipt is obtained showing (at a minimum) the identification number, the time and date of the handover, and the name and signature of the recipient. • Sending information via safe hand requires: o a unique identification number; generally, this will be a receipt number o that information be in a security briefcase (see the SCEC-Security Equipment Guide on Briefcases for the carriage of security classified information on GovTEAMS) or an approved mailbag (for information, see the SCEC-approved security equipment evaluated product list), and o that information be retained in personal custody. **Entity Safe Hand** Entity safe handing is where all of the authorised persons in the chain are officers of the entity dispatching the information. **Safe Hand Endorsed Couriers** SCEC is responsible for the SCEC-endorsed Courier Scheme. This scheme endorses commercial courier companies to safe hand courier services. All SCEC-endorsed courier companies are assessed against the SCEC endorsement criteria—safe hand courier services A11996502 - June 2018. Safe hand via an endorsed courier provides a level of assurance for the confidentiality of information being transferred, where it is not possible to use entity personnel to carry the information. There are two safe hand categories for couriers: • Safe hand courier service BIL 4 is for transporting and delivering consignments directly to a government entity consignee. It is to be used for transporting information classified up to and including SECRET. • Safe hand courier service BIL 5 is for transporting and delivering consignments directly to a government entity officer. It is to be used for transporting information classified TOP SECRET. SCEC-endorsed courier services may carry paper-based information and technology assets within Australia. This does not include weaponry and explosive ordnance (including those with controlled cryptographic items). • Safe hand courier services are not suitable for transferring valuable or attractive assets such as pharmaceuticals or money. • Special arrangements, such as armed escorts may be necessary in certain circumstances. • Some security caveated information is precluded from transfer by a commercial safe hand courier. See the Australian Government Security Caveat Standard for details. Contact ASIO-T4 via the Contact Us form, visit Couriers | Security Construction and Equipment Committee (SCEC) or see the ASIO-T4 Protective security circular (PSC) 172

Method	Description
	(available on a need-to-know basis on GovTEAMS) for advice on SCEC-endorsed safe hand courier services.

See ISM's Guidelines for Data Transfers for controls for manual data transfers and data transfers using gateways or Cross Domain Solutions. For data transfers using gateways or CDSs, the content filtering section of the Guidelines for Gateways is also applicable.

9.3.3.2. Transmit Security Classified Information

Transmit means to communicate or send information in electronic form to another entity (or person). Electronic form is when information is sent or communicated over the internet through a secure network infrastructure (i.e. OFFICIAL: Sensitive, PROTECTED, SECRET or TOP SECRET networks) or over public network infrastructure and unsecured spaces. Examples of electronic transmission include using email, facsimile, instant messaging services, GovTEAMS, telephone and videoconference.

Examples of transmitting information include:

- emailing information to a person within the entity or in a different entity, or
- verbally communicating information to a person within the entity or another entity (e.g. by telephone or videoconference).

Information is at increased risk when electronically transmitted, particularly when information is transmitted outside of a controlled environment (e.g. when an entity does not have control over the entire transmission network).

Encryption can be used to assist in protecting information from compromise where insufficient physical security is provided for the protection of information communicated over network infrastructure.

Table 22 details the minimum protections to deter and detect compromise when transmitting information electronically. See ISM for detailed guidance on protecting transmissions over networks, including information on cryptography.

Table 22: Minimum Network and Encryption Levels for Transmitting Information Electronically

Security Classification	Minimum Protections
TOP SECRET (and SECRET Codeword)	• Communicate information over TOP SECRET secure network. • Use ASD's High Assurance Cryptographic Equipment to encrypt TOP SECRET information for any communication that is not over a TOP SECRET network.
SECRET	• Communicate information over SECRET secure networks (or networks of higher classification). • Use ASD's High Assurance Cryptographic Equipment to encrypt SECRET information for any communication that is not over a SECRET network or network of higher classification.
PROTECTED	• Communicate information over PROTECTED networks (or networks of higher classification). • Encrypt PROTECTED information for any communication that is not over a PROTECTED network or network of higher classification.
OFFICIAL: Sensitive	• Communicate information over OFFICIAL: Sensitive networks (or networks of higher classification). • Encrypt OFFICIAL: Sensitive information transferred over public network infrastructure, or through unsecured spaces (including Zone 1 security areas), unless the residual security risk of not doing so has been recognised and accepted by the entity. • Consider other security measures or mitigating protections already in place, such as: o validating the recipient's address before sending information in an unencrypted form, and o sending large amounts of non-sensitive information as an encrypted or password protected attachment. Australian Privacy Principle 11 imposes additional obligations regarding the transmission of 'personal information' (as defined under the *Privacy Act*); the OAIC's Guide to Securing Personal Information provides guidance on the reasonable steps that entities may be required to take under the *Privacy Act* to protect the personal information they hold, including when such information is being transferred or transmitted.
OFFICIAL	While encryption of OFFICIAL information (as opposed to OFFICIAL: Sensitive information) is not a mandated requirement, entities are required to implement operational controls for all information holdings proportional to their value, importance and sensitivity. • Communicate information over public network infrastructure or through unsecured spaces (including Zone 1 security areas). • Transmit by means that deter and detect compromise recommended. • Encryption recommended.

9.3.4 Exceptional Circumstances and Incidents Involving Security Classified Information

Exceptional situations or emergencies may arise that prevent application of this policy. For further information on handling exceptional circumstances see PSPF Guidelines:

- Section 8.1—Exceptional Circumstances, for when and how to use this provision
- Section 4—Protective Security Reporting, for taking a risk-managed approach to implementation of PSPF requirements
- Section 3.6.4—Externally Reportable Security Incidents and Referral Obligations, for guidance on how to report unmitigated security risks to entities affected by the risk and relevant authorities

Any compromise of security classified information is considered a security incident. In accordance with PSPF Requirement 0028, if the compromise is considered significant or results in unmitigated security risks that affect another entity or authority, it may also trigger external reporting obligations.

PSPF Release 2024 (Table 2) mandates the specific timeframes in which entities must meet these reporting obligations. Where not specified, entities should report:

- compromise of security classified information to the information's originator as soon as practicable, and
- matters relating to national security (such as compromise of SECRET or TOP SECRET information) to the Director-General, ASIO as soon as possible after the compromise is detected.

9.4 Information Management Markers

Information management markers (IMMs) 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.

Table 23: Assessing whether to use an Information Management Markers

IMM	Description	Restrictions	Notes
Legal Privilege	Information is subject to legal professional privilege.	• Restrictions on access to, or use of, information covered by legal professional privilege. • Apply with security classification (recommended).	Compromise of the confidentiality of information subject to legal professional privilege is likely to cause at least limited damage to the national interest, organisations or individuals.
Legislative Secrecy	Information is subject to one or more legislative secrecy provisions. Legislative secrecy provisions impose confidentiality obligations on individuals or entities.	• Restrictions on access to, or use of, information covered by specific legislative secrecy provisions. • Apply with a warning notice that informs the recipient of relevant provisions (required). • Apply with security classification (recommended).	Compromise of the confidentiality of information subject to legislative secrecy provisions is likely to cause at least limited damage to the national interest, organisations or individuals. The legislative secrecy IMM is used to draw attention to the applicability of one or more specific secrecy provisions. This is achieved by means of a warning notice placed at the top or bottom of each page of a document or in the body of an email that expressly identifies the specific secrecy provisions under which the information is covered.
	Examples of warning notices: • Legislative Secrecy Warning: Unless you have written consent from the [insert authority or relevant position], it is an offence under section XX of the XXX Act to [insert details of restrictions]. • This information is subject to [insert reference to section of relevant legislation]. Compromise or improper handling of this information may result in [insert relevant penalty]. This information can only be incorporated in other material which bears the legislative secrecy IMM and contains this warning notice.		
Personal Privacy	Information is personal information as defined in the *Privacy Act 1988*	• Restrictions under the Privacy Act on access to, or use of, personal information collected for business purposes.	The Privacy Act requires entities to protect the personal information they hold from misuse, interference, loss, and from unauthorised access, modification or disclosure.

IMM	Description	Restrictions	Notes
		• Apply with security classification (recommended).	

Privacy Act Definitions

- Personal information: information or an opinion (including information or an opinion forming part of a database), whether true or not, and whether recorded in a material form or not, about an individual whose identity is apparent, or can reasonably be ascertained, from the information or opinion. See What is 'personal information'? | ALRC for further guidance.
- Sensitive information: includes personal information about an individual's:
  - racial or ethnic origin
  - political opinions
  - membership of a political organisation
  - religious beliefs or affiliations
  - philosophical beliefs
  - membership of a professional or trade organisation or trade union
  - sexual orientation or practices
  - criminal record
  - health or genetic information about an individual that is not otherwise health information, or
  - some aspects of biometric information.

See Sensitive information | ALRC for further guidance.

The Privacy Act generally affords a higher level of privacy protection to sensitive information than to other personal information.

9.5 Security Caveats and Accountable Material

9.5.1 Security Caveats

Security caveats are a warning that the information has special protections and handling requirements in addition to those indicated by the security classification. Each security caveat is governed by a 'controlling authority', which is responsible for managing the security caveat and establishing the additional special protections and handling requirements beyond those imposed by the security classification. PSPF Requirement 0063 mandates that the special handling requirements imposed by the controlling authority are applied to protect caveated information.

Security caveats are not classification and in accordance with PSPF Requirement 0064, must be clearly marked as text and only appear with a security classification of PROTECTED or higher. The originator's approval is required to remove a security caveat. See PSPF Guidelines Section 9.1.1—Sanitisation, Reclassification or Declassification.

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.

The Australian Government Security Caveat Standard (available on need-to-know basis on GovTEAMS) defines the security caveats used by the Australian Government and details the mandatory elements for protecting and handling security caveated information and accountable material. Table 24 describes the most commonly used security caveats.

Table 24: Commonly Used Security Caveats

Caveat Category	Caveat Coverage	Special Handling Requirements
Codewords (sensitive compartmented information)	Use of codewords is primarily within the national security community. A codeword indicates that the information is of sufficient sensitivity that it requires protection in addition to that offered by a security classification. Each codeword identifies a special need-to-know compartment. A compartment is a mechanism for restricting access to information by defined individuals who have been 'briefed' on the particular sensitivities of that information and any special rules that may apply. The codeword is chosen so that its ordinary meaning is unrelated to the subject of the information.	It may be necessary to take precautions beyond those indicated by the security classification to protect the information. These will be specified by the entity that owns the information, for instance those with a need to access the information will be given a special briefing first.
Foreign government markings	Foreign government markings are applied to information created by Australian entities from foreign source information.	PSPF Requirement 0082 requires that where an international agreement or international arrangement is in place, entities must safeguard security classified foreign entity information or resources in accordance with the provisions set out in the agreement or arrangement. Foreign government marking caveats require protection at least equivalent to that required by the foreign government providing the source information.
Special handling instructions	Use of special handling instructions is primarily within the national security community. Some special handling instructions are used more broadly across government, as follows:	Special handling instructions indicate particular precautions for information handling.
	EXCLUSIVE FOR (named person) The EXCLUSIVE FOR caveat identifies information intended for access by a named recipient only.	Access to EXCLUSIVE FOR information is limited to a named person, position title or designation.
	CABINET The CABINET caveat identifies any information that: • is prepared for the purpose of informing the Cabinet • reveals the decision and/or deliberations of the Cabinet • is prepared by departments to brief their ministers on matters proposed for Cabinet consideration, or • has been created for the purpose of informing a proposal to be considered by the Cabinet.	The Cabinet Handbook - 15th edition specifies handling requirements for Cabinet documents. This includes applying a security classification of at least PROTECTED to all Cabinet documents and associated records.
Releasability caveats	There are three releasability caveats used across government:	Releasability caveats limit access to information based on citizenship.
	Australian Eyes Only (AUSTEO) The AUSTEO caveat indicates only appropriately cleared Australian citizens can access the information. Additional citizenships do not preclude access.	Information marked AUSTEO is only passed to, or accessed by, Australian citizens. While a person who has dual Australian citizenship may be given AUSTEO-marked

Caveat Category	Caveat Coverage	Special Handling Requirements
		information, in no circumstance may the Australian citizenship requirement be waived.
	Australian Government Access Only (AGAO) The AGAO caveat indicates information that can only be accessed by appropriately cleared Australian citizens and appropriately cleared representatives of Five-Eyes Governments on exchange, secondment, long-term posting or attachment within the National Intelligence Community, the Department of Defence and the Australian Submarines Agency.	AGAO information must not be distributed to the Five Eyes foreign representative's parent agency or government. AGAO information may not be shared with any other foreign nationals. Where appropriate, all entities may apply the AGAO caveat to classified information. However, entities other than members of the National Intelligence Community, Department of Defence and the Australian Submarines Agency must handle AGAO material as if it were marked AUSTEO.
	Releasable To (REL) The Releasable To (REL) caveat identifies information that has been released or is releasable to citizens of the indicated countries only. Countries are identified using three letter country codes from International Standard ISO 3166-1:2013 Codes for the representation of names of countries and their subdivisions – Alpha 3 codes.	For example, REL AUS/CAN/GBR/NZL/USA means that the information may be passed to citizens of Australia, Canada, United Kingdom, New Zealand and the United States of America only. The caveat is an exclusive marking that disqualifies a third-party national seconded or embedded in an Australian or foreign government entity from accessing the information.

The NATIONAL CABINET security caveat is being phase out as National Cabinet is no longer a committee of Cabinet. Entities are encouraged to remove this security caveat from use.

9.5.2 Accountable Material

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

What constitutes accountable material may vary from entity to entity and could include budget papers, tender documents and sensitive ministerial briefing documents.

Information that is accountable material by default includes:

- TOP SECRET information
- All codeword information
- Select special handing instruction caveats
- Any classified information designated as accountable material by the originator.

PSPF Requirement 0066 mandates that the special handling requirements imposed by the controlling authority are applied to protect accountable material. The originator's approval is required to remove, copy or amend accountable material. See PSPF Guidelines Section 9.1.1—Sanitisation, Reclassification or Declassification.

Accountable material requires the originating entity to keep accurate records and control distribution, including:

- Reference number (PSPF Requirement 0065), a unique identifier assigned to the accountable material that differs from an information management system file reference. For example, [internal reference such as section, project or program acronym]-[year]-[document number], PSPF-2024-125.

- Reference numbers should be sequential and commence at the number one for the first entry in the auditable record. See Information Asset Registers for further information and examples.

- Page numbering (PSPF Requirement 0065), a sequence of numbers to track how many pages the accountable material comprises. For example, Page 3 or 10.
- Auditable register (PSPF Requirement 0072), to maintain a complete record of all accountable material holdings, including creation, distribution, receipt and disposal. For example a classified document register. See Information Asset Registers for information and further examples.
    - The auditable register is also required to track the number of copies received or produced for accountable material.

9.6 Email Protective Marking Standard

PSPF Requirement 0067 mandates that 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.

The Australian Government Email Protective Marking Standard details the standardised format for protective markings, security classifications, security caveats and, where relevant information management markers, on emails exchanged in, and between Australian Government entities, and with 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.

For emails, the preferred approach for the Australian Government is to apply protective markings to the internet message header extension, in accordance with the Australian Government Email Protective Marking Standard. This helps with construction and parsing by email gateways and servers, and allows for information handling based on the marking or security classification.

Where an internet message header extension is not possible, the marking or security classification is placed in the subject field of an email.

See PSPF Guidelines Section 14.4—Mark Inbound Emails from External Organisations.

Figure 11: Example of Email Marking

When printed, an email is considered a physical document, as such, a visual presentation of the protective marking (such as a separate line in the email) is important.

9.7 Recordkeeping Metadata Standard

Metadata is a term used for '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.

Entities must apply the Australian Government Recordkeeping Metadata Standard to protectively mark information on systems that store, process, or communicate OFFICIAL or security classified information.

PSPF Requirement 0068 mandates that 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.

- Security classification property—identifies the security classification of the information and is used to identify information that is restricted to users with appropriate security clearance permissions.
- Security caveat property—used with the security classification property, this property identifies that the information requires additional special handling and that only people cleared and briefed to see it may have access.

PSPF Requirement 0069 mandates that the Australian Government Recordkeeping Metadata Standard's 'Rights' property where the entity wishes to categorise information content by the type of restrictions on access.

- Rights property— optional property to identify non-security related restrictions on the use or access to records. The National Archives of Australia has established a subset of rights property terms for common usage as information management markers to categorise information.

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 (available to government personnel on GovTEAMS) defines 'irregular discussions' as those that are unpredictable, non-ongoing or unannounced.

Consistent with PSPF Requirement 0189, entities are to consider the need to conduct security classified discussions throughout the process of planning, selecting, designing and modifying their facilities, to ensure the required physical security measures can be accommodated with the facilities. For guidance see ASIO Technical Note 1/15 – Physical Security of Zones, Section 16—Audio Security.

When designing an audio secure room suitable for security classified discussions, entities should consider a number of factors that may influence the specification and construction techniques used, including:

- the security classification of information being discussed, and
- the regularity of discussions.

9.8.1 Approved Locations for Security Classified Discussions

PSPF Requirement 0070 mandates that the security classification discussions and dissemination of security classified information may only take place in approved locations.

Table 25 details the approved locations for security classified discussions and dissemination of security classified information. When a location requires entities to 'exercise judgement', use discretion to judge the suitability of the location, including the environment and who else can hear the security classified information.

Table 25: 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[11]	Yes	Yes
Zone 4	No, but ASIO Technical Notes permit irregular discussions	Yes	Yes	Yes
Zone 5	Yes	Yes	Yes	Yes
Outside entity -public spaces	No	No	No[12]	Yes, but exercise judgement
Outside entity – home based work	No[12]	No[12]	Yes, but exercise judgement	Yes, but exercise judgement
While travelling	No[12]	No[12]	No[12]	Yes, but exercise judgement

Locations where security classified discussions will take place require proportionate physical and audio security measures to prevent deliberate or accidental overhearing. 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.

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.

It may be operationally critical to hold security classified conversations where an audio secure room is not available. In such cases, it is recommended that these conversations are not held in public places or where the conversation may be overheard, for example hire cars, hotel rooms, airport lounges, aeroplanes or cafes.

PSPF Requirement 0210 mandates that Technical Surveillance Countermeasures (TSCM) are established for Security Zones One to Five in accordance with the physical security measures and controls for technical surveillance countermeasures, see PSPF Release 2024 (Table 48) for mandatory elements. See PSPF Section 25.9—Technical Surveillance Countermeasures for guidance on protecting security classified discussions from technical compromise.

[11] ASIO Technical Notes define 'irregular discussions' as those that are unpredictable, non-ongoing or unannounced.
[12] 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.

9.9 Historical Classifications

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

Table 26: Historical Markings and Classifications

Historical Marking or Classification	Key Dates	Current Equivalency	Handling
CONFIDENTIAL classification	Ceased on 1 October 2020	• None established. • Consider the harm and apply corresponding security classification	Historical handling protections remain. See Table 28 for Protection and handling of CONFIDENTIAL information
For Official Use Only (FOUO) dissemination limiting marker (DLM)	Ceased on 1 October 2020	• OFFICIAL: Sensitive security classification	Handle as per OFFICIAL: Sensitive information
Sensitive DLM	Ceased on 1 October 2020	• OFFICIAL: Sensitive, unless otherwise security classified	Handle as per OFFICIAL: Sensitive information, unless otherwise classified
Sensitive: Cabinet DLM	Ceased on 1 October 2020	• CABINET security caveat applied in conjunction with a security classification of PROTECTED or higher	Handle as per: • Specified security classifications, and • Australian Government Security Caveat Standard requirements for the CABINET security caveat
Sensitive: Legal DLM	Ceased on 1 October 2020	• OFFICIAL: Sensitive, unless otherwise security classified • The (optional) *Legal privilege* information management marker may be applied	Handle as: • specified security classification, or • OFFICIAL information, if not classified
Sensitive: Personal DLM	Ceased on 1 October 2020	• OFFICIAL: Sensitive, unless otherwise security classified • The (optional) *Personal privacy* information management marker may be applied	Handle as per: • specified security classification, or • OFFICIAL information, if not classified
HIGHLY PROTECTED classification	Ceased on 1 August 2012	• SECRET security classification	Handle as per SECRET information
RESTRICTED classification	Ceased on 1 August 2012	• OFFICIAL: Sensitive security classification	Handle as per OFFICIAL: Sensitive information
X-IN-CONFIDENCE classification	Ceased on 1 August 2012	• OFFICIAL: Sensitive security classification	Handle as per OFFICIAL: Sensitive information

9.9.1 Protection and handling of CONFIDENTIAL information

The historical classification CONFIDENTIAL does not have an equivalent level of classification under the current PSPF. Information that was classified as CONFIDENTIAL before October 2020 has a business impact level of very high. This means that the compromise of CONFIDENTIAL information's confidentiality would be expected to cause significant damage to the national interest, organisations or individuals. Table 27 provides the sub-impact categories for this business impact level.

Table 27: Business Impact Level of CONFIDENTIAL information: Business Impact Level 3A

Sub-Impact Categories	Significant Damage Is:
Impacts on national security	• causing damage to national security
Impacts on entity operations	• causing a severe degradation in, or loss of, organisational capability to an extent and duration that the entity cannot perform one or more of its functions for an extended time • resulting in major long-term harm to entity assets
Australian financial and economic impacts	• undermining the financial viability of, or causing substantial financial damage to, a number of major Australia-based or Australian-owned organisations or companies • causing long-term damage to the Australian economy to an estimated total of $10 to $20 billion • causing major, short-term damage to global trade or commerce, leading to short-term recession or hyperinflation in Australia
Impacts on government policies	• significantly disadvantaging Australia in international negotiations or strategy • tempo vulnerability disclosure program rarely damaging the internal stability of Australia or friendly countries • causing significant damage or disruption to diplomatic relations, including resulting in formal protest or retaliatory action
Impacts on personal safety	• endangering small groups of individuals – the compromise of information could lead to serious harm or potentially life-threatening injuries to a small group of individuals
Impacts on crime prevention	• causing major, long-term impairment to the ability to investigate serious offences, i.e. offences resulting in two or more years imprisonment
Impacts on Defence operations	• causing damage to the operational effectiveness or security of Australian or allied forces that could result in risk to life
Impacts on intelligence operations	• causing damage to Australian or allied intelligence capability
Impacts on national infrastructure	• damaging or disrupting significant national infrastructure

The following information describes the minimum protections and handling requirements for legacy CONFIDENTIAL information.

Table 28: Minimum Protections and Handling Requirements for CONFIDENTIAL Information

BIL 3.5	CONFIDENTIAL—significant damage to the national interest, organisations or individuals
Text-based marking	Maintain text-based protective marking CONFIDENTIAL to documents (including emails). From October 2020, do not mark new information as CONFIDENTIAL. For new information that would previously have been marked CONFIDENTIAL, consider the harm and apply corresponding security classification marking under the current PSPF.
Alternative marking	If text-based markings were not used, maintain colour-based markings. For CONFIDENTIAL a green colour was used historically. If text or colour-based protective markings cannot be used, apply the entity's marking scheme for such scenarios.
Paragraph marking	Optional. (CONFIDENTIAL) or abbreviated to (C)
Access control	Need-to-know principle: Yes. Security clearance: NV1 (minimum). Temporary access: NV1 (minimum), supervised.
Use – Zones 1 to 5	CONFIDENTIAL information and mobile devices that process, store or communicate CONFIDENTIAL information can be used in security Zones 1-5.

Use – Outside entity facilities	No, do not use outside entity facilities.
Use – Home based work	Regular: No. Occasional: Not recommended, but if required, obtain manager approval, apply entity procedures on need for a security assessment, and exercise judgement to assess environment risk
Leave unattended	No, store securely when unattended.
Store – Zone 1	No, do not store
Store – Zone 2	Yes, Class B container
Store – Zones 3 to 5	Yes, Class C container
Store – Outside entity facilities	Not recommended. If required for occasional home-based work (see use above): • apply requirements for carrying outside entity facilities, and • retain in personal custody (strongly preferred), or for brief absences from home, store in Class B container or higher container (container must be approved as a proper place of custody by the Accountable Authority or their delegate), and return to entity facility as soon as practicable
Carry – Zone 1	Physical CONFIDENTIAL information inside entity facilities - retain in personal custody in an opaque envelope or folder that indicates classification and place in a security briefcase, pouch or satchel.
Carry – Zones 2 to 4	Physical CONFIDENTIAL information inside entity facilities - retain in personal custody in an opaque envelope or folder that indicates Classification Mobile device that processes, stores or communicates CONFIDENTIAL information inside entity facilities - carry in secured state; if in an unsecured state, apply entity in procedures
Carry – Zone 5	Physical CONFIDENTIAL information inside entity facilities - retain in personal custody in an opaque envelope or folder that indicates Classification Mobile device that processes, stores or communicates CONFIDENTIAL information inside entity facilities - if in a secured or unsecured state, apply entity procedures
Carry – Outside entity facilities	Physical CONFIDENTIAL information outside entity facilities (including external meetings) and between entity facilities: • retain in personal custody • place in a security briefcase, pouch or satchel, and • recommend tamper-evident packaging if aggregate information increases risk. Mobile device that processes, stores or communicates CONFIDENTIAL information outside entity facilities (including external meetings) and between entity facilities: • in a secured state, retain in personal custody • in an unsecured state, carry inside a security briefcase, pouch or satchel and consider tamper evident seals.
Transfer – Inside entity facilities	inside entity facilities (Zones 1-5): transfer by hand or entity safe hand and apply requirements for carrying; can be uncovered if office environment presents very low risk of unauthorised viewing
Transfer – Different facility	Transfer to another officer in a different facility: • apply requirements for carrying outside entity facilities, and • transfer by hand, entity safe hand, safe hand courier rated BIL 4, or DFAT courier (if transfer by courier, use tamper evident packaging). Any transfer requires a receipt.
Transmit	When transmitting electronically communicate over SECRET secure networks (or networks of higher classification). Use ASD's High Assurance Cryptographic Equipment to encrypt CONFIDENTIAL information for any communication that is not over a SECRET network (or network of higher classification).

Travel – in Australia	When travelling with physical CONFIDENTIAL information: • apply requirements for carrying outside entity facilities and any additional entity procedures • for airline travel, retain as carry-on baggage and if airline requires to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim ASAP • do not leave CONFIDENTIAL information unattended, retain in personal custody, and • do not store while travelling (e.g. in a hotel room), if storage required, store in an Australian entity facility. When travelling with a mobile device that processes, stores or communicates CONFIDENTIAL information: • apply requirements for carrying outside entity facilities and any additional entity procedures • not recommended for airline travel, if required, retain as carry-on baggage and if airline requires to be checked at the gate, try to observe entering and exiting the cargo hold and reclaim ASAP • do not leave CONFIDENTIAL information unattended, retain in personal custody, and • do not store while travelling, if storage required, store in an Australian entity facility.
Travel – International	Not recommended to travel overseas with physical CONFIDENTIAL information. If required, follow entity procedures, and if required, consult DFAT. Do not travel overseas with a mobile device that processes, stores or communicates CONFIDENTIAL information. If required, see DFAT advice on options to access information at destination.
Dispose	Dispose of CONFIDENTIAL information using a Class A shredder or entity-assessed and approved or NAID AAA certified destruction service with specific endorsement and approved equipment and systems.

10 Information Holdings

Information is a valuable asset. Information is an encompassing term for 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.

PSPF Requirement 0071 mandates that entities implement operational controls for it information holdings that are proportional to their value, importance and sensitivity. This process applies equally when information is aggregated or integrated to form a new holding.

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

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.

Table 29 provides a suggested process for assessing the value, importance and sensitivity of aggregated or integrated holdings.

Table 29: Process for Considering the Security Classification of Aggregated or Integrated Holdings

Process steps	Things to consider

Identify aggregated or integrated holdings	Identify the aggregated or integrated holdings in your entity, and give thought to the following:
	• Has the information been sanitised or declassified from the original source?
	• Where is the holding stored and on what type of technology system?
	  o Is the system authorised to operate and with sufficient access and security controls?
	  o If stored on a legacy system, are there sufficient alternative mitigations in place to limit the compromise of this data?
	  o If stored on an IT or technology system that connects to multiple other systems, are the access controls in place sufficient to prevent unauthorised access to the dataset?
	  o Does the system have sufficient access controls?
	• What permissions are in place to hold, store or use the holding? Will you need to agree the appropriate classification and/or protections with another entity?

Assess the value, importance or sensitivity	Assess the security classification of the holding, and decide the classification by considering the potential damage to the government, national interest, organisations or individuals, that would arise if the holding's confidentiality was compromised. Give thought to the following: • What is the highest classification or marking present in the holding?

Process steps	Things to consider
	• Does the collated information reveal new and more sensitive information or intelligence than would be apparent from the main source records that would cause greater damage than individual documents? • Does bringing this information together make it a more attractive target to a potentially malicious actor or trusted insider? For example, large amounts of OFFICIAL: Sensitive personal or corporate information that when aggregated reveal significant information about the entity's operations or personnel. • Does other information or data stored on the same system affect the value of the holding? • Does the holding include caveated[13] information or optional information management markers and will this affect or limit the options for aggregating or integrating this information?
Consider the options and constraints	Based on the information gathered in the first two steps, consider the options available to your entity and any constraints that would affect the appropriate classification to apply. Give thought to the following: • If the aggregated holding's classification is required to be raised, will it remain on the same system, where the same users will be able to access the information? If so, consider whether additional access or security controls are required to protect the aggregated information holding. • Does your entity's risk environment make your information a more attractive target for compromise by a malicious actor, including a trusted insider? If so, does this affect the type of access or security controls you will implement to protect the holding or does the holding need to be moved to a technology system that enforces additional access requirements? • What is your internal security environment? Will the holding only be accessed by security cleared personnel, including any contractors? • What are the classifications of the technology systems you have available to store the holding? • Where the entity does not have access to a technology system rated to the proposed classification of the holding, remedial action is required to ensure the commensurate requirements for that classification can be implemented. o This may mean removing or storing the highly classified components separately. For example, if the holding is assessed overall as SECRET but the entity only has access to a PROTECTED network, then action will be required to ensure the holding is assessed no higher than PROTECTED. This may mean removing the more highly classified components.
Decide and document	Decide which protective marking or security classification to apply and what, if any, additional access or security controls are required to protect the holding from compromise. Document the decision in the entity's security plan along with acceptance of any residual risk and period of review of the decision.

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.

PSPF Requirement 0071 mandates that an auditable register is maintained for TOP SECRET information and accountable material. Entities are also recommended to:

- keep an audit log or register for documents at other classification levels (particularly for SECRET information), or registered information received from other entities

[13] Refer to the Australian Government Security Caveat Guidelines for classification and handling requirements.

- develop procedures for regular spot checks to ensure accountable material (including TOP SECRET information) is accounted for and being handled, used and stored appropriately, and
    - For example, do a spot check to sight 5 per cent of TOP SECRET files per month, with 100 per cent of TOP SECRET files checked within a two-year period.
- use receipts for transfer of all physical security classified information. Receipts can be used to identify the date and time of dispatch, the dispatching officer's name and a unique identifying number. Additionally, receipts can be used as a mechanism to control the incoming transfer of information (e.g. a two-part receipt placed in the inner envelope with the information means the addressee can keep one portion and sign and return the other to the sender).

There may be other legislative requirements for record keeping. For example, under the Privacy (Australian Government Agencies – Governance) APP Code 2017, a Privacy Officer is required to maintain a record of an entity's personal information holdings and a register of privacy impact assessments.

See PSPF Guidelines Section 9.5—Security Caveats and Accountable Material.

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 it is destroyed. 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.

PSPF Requirement 0073 mandates that OFFICIAL and security classified information is disposed of securely in accordance with the Minimum Protections and Handling Requirements, ISM, the Records Authorities, a Normal Administrative Practice and the *Archives Act 1983*. PSPF Requirement 0074 mandates that security classified information is appropriately destroyed in accordance with the Minimum Protections and Handling Requirements when it has passed minimum retention requirements or reaches authorised destruction dates.

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.

Destruction of Australian Government information can occur if it is:

- approved by a records authority
- required by legislation
- covered under a normal administrative practice (NAP).

The National Archives of Australia's (National Archives) Information Management Standard for Australian Government Principle 6 states *that business information is accountably destroyed or transferred,* and recommends the following actions:

- Assess business information against current records authorities - Records authorities set out the minimum periods that business information should be retained.
- Confirm there is no need to keep business information beyond the authorised retention period. Some business information will have long-term historical and social value. Examples of where information may require retention:
    - anticipated requests for access
    - likely legal action
    - a significant increase in public interest in the topic, or
    - a disposal freeze issued by the National Archives for business information on that issue or event.
- Follow any protective security requirements for destruction, including:
    - PSPF Minimum Protections and Handling Requirements
    - ASD's ISM
    - National Archives' Compliant destruction of Australian Government records
- Document the action, authority and approval for destruction or transfer.

There may be other legislative requirements that apply to the disposal of information. For example, Australian Privacy Principle 11.2 imposes obligations on the destruction and de-identification of personal information under the Privacy Act.

11.1 Destroy Security Classification Information

A variety of methods can be used for the secure destruction of information in physical form.

ASIO-T4 approves specifications for equipment used to destroy physical security classified information. Commonly used destruction methods include:

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

The ISM provides guidance on sanitisation and destruction of IT equipment and storage media. Methods for destroying digital information include:

- digital file shredding
- degaussing by demagnetising magnetic media to erase recorded data
- physical destruction of storage media through pulverisation, incineration or shredding, or
- reformatting, if it can be guaranteed that the process cannot be reversed.

Commercial providers may be used to destroy security classified information. Consider the appropriateness of a commercial provider's collection process, transport, facility, procedures and approved equipment when considering external destruction services. These considerations can be made against ASIO-T4 Criteria – agency-assessed and approved destruction service (available on a need-to-know basis on GovTEAMS).

Appropriate procedures include ensuring:

- security classified information is attended at all times and the vehicle and storage areas are appropriately secured
- that destruction is performed immediately after the material has arrived at the premises
- that destruction of security classified information is witnessed by an entity representative, and
- destruction service staff have a security clearance to the highest level of security classified information being transported and destroyed, or appropriately security cleared entity staff escort and witness the destruction.

A number of commercial providers hold National Association for Information Destruction AAA certification for destruction service (with endorsements as specified in PSC 167 External destruction of security classified information – available on a need-to-know basis on GovTEAMS). These commercial providers are able to destroy security classified information.

Information classified TOP SECRET or accountable material should be destroyed within entity premises; the originating entity may request notification of destruction. The originator of some accountable material may apply special handling conditions that prevent information destruction being contracted out.

12 Information Sharing

PSPF Requirement 0075 mandates that 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, to reduce the risk of unauthorised disclosure, and is transferred in accordance with the Minimum Protections and Handling Requirements.

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

See PSPF Guidelines Section 17.1—Temporary Access to Resources.

12.1 Need-to-Know Principle

The need-to-know principle applies to all security classified information. It reflects the need for personnel to access this information only where there is an operational requirement to do so.

In accordance with PSPF Requirement 0075 access to, and dissemination of, security classified information is limited to personnel who need the resources to do their work. Meaning if a person requires the information or access to the resource to do their job or fulfil a function, then they have a need-to-know.

This involves:

- providing access to information only to personnel who need that access; not based on convenience or because of their status, position, rank or level of authorised access, and
- a positive obligation to share relevant information so that people with an operational need-to-know the information have access.

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.

However, having a security clearance and a need-to-know are not the only factors to consider when sharing security classified information. The subsequent sections in this chapter outline other requirements for sharing information across and outside of government.

12.2 Domestic Information Sharing

Domestic information sharing covers official information shared within Australia to both government and non-government stakeholders.

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.

PSPF Requirement 0076 mandates that the MOU is applied when sharing information with State and Territory government agencies. 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.

The MOU remains valid until a new MOU is negotiated between all parties. The MOU refers to 'National Security Information', which covered SECRET and TOP SECRET information along with several classifications that have now ceased. Under the PSPF this terminology equates to security classified information.

The MOU is available to those with a need-to-know on GovTEAMS.

12.2.3 Sharing with Non-Government Stakeholders

PSPF Requirement 0077 mandates 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.

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.

Agreements for information disclosure provide assurance that external stakeholders understand the obligations to protect government information and resources. Legislative provisions on access to information

In addition, under some legislation, it may be necessary to limit sharing of information depending on the purpose for which it was collected. For example, secrecy provisions, privacy law and legal professional privilege restrict information access in some cases. It may be an offence under the *Crimes Act 1914* or *Criminal Code Act 1995* to share or disclose information inappropriately.

Some government policy and legislation may also require agreement or consent to disclose information (e.g. sharing classified personal information covered by Australian Privacy Principles).

Consider the following factors before sharing information:

- Is the information is subject to section 95B of the Privacy Act? This section mandates that entities take contractual measures to ensure that a contracted service provider does not do an act, or engage in a practice, that would breach an Australian Privacy Principle.
- Is the information is subject to any legislative secrecy provisions?
- Does the aggregation of information to be shared increases the business impact level of potential compromise? If so, the access and security clearance requirements will also be elevated.
- What type of access is being granted and what level of supervision and control will the entity have over the personnel granted access.

PSPF Requirement 0077 applies to external parties accessing, processing, communicating, storing or managing security classified information and resources, and/or providing products, services or functions to the entity. See Third Party Risk Management for guidance on managing and monitoring these arrangements.

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

12.3 International Information Sharing

12.3.1 Provisions for International Information Sharing

PSPF Requirement 0079 requires an explicit legislative provision, international agreement or arrangement to be in place for a foreign national or entity to access Australian Government security classified information.

The Australian Government takes a considered approach to international information sharing agreements and arrangements. There are generally two types of agreements:

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

Whole of government international agreements are typically called or referred to as General Security Agreements. Existing whole of government international agreements for the protection of security classified information between Australia and various countries or international organisations (for example the European Union or the Organisation for Joint Armament Cooperation) where security classification equivalencies and protections have been established. See Australian Treaty Series for details.

PSPF Requirement 0079 prevents sharing of Australian Government security classified information and resources with a foreign entity unless an explicit legislative provision, international agreement or arrangement for its protection are in place.

It may be an offence under the *Crimes Act 1914* or *Criminal Code Act 1995* to share information with a foreign entity inappropriately.

The standard processes for sharing Australian Government security classified information and resources with a foreign entity or person includes:

- establishing or utilising an international agreement or arrangement with a foreign government or international organisation that includes provisions for the protection and handling of security classified information or resources
- obtaining appropriate authorisation prior to sharing information or assets (approval at the Senior Executive Service level is recommended)
- making the purpose of the information or asset sharing clear, i.e. the reason for sharing
- keeping a record of the information or resource transfer (including meeting PSPF Requirement 0072 to maintain an auditable register for TOP SECRET information and accountable material)
- maintaining a register, where appropriate, of all Australian Government security classified information and resources shared, even if a register is not prescribed in the agreement or arrangement
    - the register is recommended to include the date of sharing, recipient of the information or resources, description and classification of the information or resources shared.

Recommended Approach

- ✔ Establish sound record keeping procedures for sharing with international stakeholders that demonstrates the appropriateness of information sharing.

12.3.2 International Stakeholder Information and Resources

In whole of government international and entity-to-entity specific agreements and arrangements, information classifications and equivalencies are established to determine the mutual protection of classified information.

Where equivalent security classifications between the foreign entity and Australian Government are established, international agreements or arrangements outline specific instructions to identify the corresponding security classification and additional protection and handling requirements.

Where information is received and not covered by an international agreement or arrangement, entities should work with the originator and the entity's security team to apply an Australian Government security classification where foreign entity information or resources. The application of an Australian Government security classification is based on an assessment of the value, importance and sensitivity of the information or asset, see PSPF Guidelines Section 9.2 for guidance of applying security classifications.

Entities should also apply the following protections:

- ensuring individuals who access foreign entity information or assets hold a security clearance at the appropriate level
- limiting access to the foreign entity information or assets to individuals with a need-to-know
- protecting the foreign entity information or assets from unauthorised access
- transmitting the information by secure means, and
- seeking approval from the originating government before releasing their information to any other foreign government or foreign entity.

In addition to the security classification, entities may need to mark foreign entity information and resources with the 'RELEASABLE TO' caveat. This identifies the source of information or resources and restricts release to certain nationalities. This caveat, and their access requirements, are outlined in Table 24. See PSPF Guidelines Section 9.5 and the Australian Government Security Caveat Standard for guidance information of security caveats and accountable material.

In accordance with PSPF Requirement 0058, an entity may only share security classified information with a foreign entity where they are the originator. Information generated outside of the entity requires the originator's approval before sharing with a foreign entity.

Entities should obtain originator agreement for third-party access to security classified information or resources. International agreements or arrangements commonly require written approval from the originator for release of security classified information or resources to any other party. If these provisions are not included in an agreement, entities should seek written approval from the originating foreign government before releasing security classified information to any other foreign government or foreign national.

Recommended Approach

- ✔ Review the relevant international agreement or arrangement to identify additional obligations or protections that may differ from the PSPF requirements.

12.3.3 International Information Sharing Governance

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.

Some agreements give particular Australian Government entities (referred to as Competent Security Authorities) responsibility for administering international agreements or arrangements in specific fields. For example, the Department of Defence is a Competent Security Authority for Defence matters.

PSPF Guidelines Section 2.3.1 details the responsibilities of the CSO. CSOs (or appropriate security practitioner delegates) investigate, respond to and report on security incidents including:

- Failing to safeguard security classified foreign entity information or assets covered by an international agreement or arrangement may be in breach or violation of PSPF Requirement 0078. Security breaches or violation incidents can involve the actual (or suspected) compromise of foreign entity classified information or assets.
- Sharing classified Australian information and resources inappropriately with a foreign national or international entity without the protection of an agreement or arrangement may be in breach or violation of PSPF Requirement 0079 and may be an offence under the *Crimes Act 1914* or *Criminal Code Act 1995*. Ensuring all instances of international information and asset sharing without agreement or arrangement are reported to the entity CSO (or appropriate security practitioner delegate) will assist security incident investigations.

International agreements or arrangements may impose additional reporting and security violation requirements beyond those detailed in the PSPF.

12.3.3.1. Ad Hoc Process for Sharing with Foreign Governments

Ad hoc or once off information sharing arrangements are permitted with foreign governments where a general security agreement or other security classified sharing arrangement is not already in place (including an entity-to-entity agreement). Ad hoc written arrangements can take a variety of forms such as formal written arrangements between entities, exchanges of letters or diplomatic notes between the Australian Government and the foreign government or international organisation.

This requires appropriate written arrangements that adhere to, and approval by the Accountable Authority, that are:

- 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
- informed by a risk assessment, and
- inclusive of the protections for use and storage of security classified and caveated information and resources in accordance with the Minimum Protections and Handling Requirements and the Australian Government Security Caveat Standards.

Recommended Approach

- ✔ Report security incidents to the originating foreign government as soon as possible.

12.3.4 Negotiating International Agreements and Arrangements

When negotiating international agreements or arrangements with foreign governments or international organisations, considerations must be made for the protection of Australian Government security classified information and resources that could or can be shared under the agreement or arrangement.

International agreements or arrangements that include sharing of Australian Government security classified information must outline protective security provisions including, but not limited to:

- marking of security classified information and resources
- protection of security classified information and resources, including how they are handled and transferred

- access to and disclosure of security classified information and resources, including personnel security clearance requirements and recognition
- responding to breaches or security violations, and
- undertaking security inspections and visits.

Entities wanting to negotiate a treaty, or an instrument of less than treaty status, including treaties or instruments that involve national security issues, must be aware of their obligations under the Legal Services Directions 2017. The Directions tie certain categories of legal work to specified providers unless approval to use a non-tied provider is obtained. This includes that legal advice preparatory to, or in the course of, treaty negotiations (which includes negotiation of instruments of less than treaty status) must be sought from the Office of International Law in the Attorney-General's Department, the Australian Government Solicitor or the Department of Foreign Affairs and Trade (as required under the Directions), unless approval is otherwise obtained. Where negotiations include provisions for sharing Australian Government security classified information, the Department of Home Affairs must also be consulted. This consultation process establishes consistent equivalencies for the protection of security classified information and resources and ensures that Minimum Protections and Handling Requirements of security classified information are met.

Entities establishing new whole-of-government or entity-to-entity agreements or other arrangements are encouraged contact the Department of Home Affairs (PSPF@homeaffairs.gov.au) to discuss international information sharing requirements.

12.3.5 Sharing with Non-Government International Stakeholders through Classified Contracts

PSPF Requirement 0077 requires that an agreement or arrangement, such as a contract or deed that establishes minimum protections and handling requirements is in place with a non-government international stakeholder before security classified information or resources are disclosed or shared with a person or organisation outside of the Australian Government.

In addition, PSPF Requirement 0083 states that 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 the protection of classified information and resources are in place. These international agreements or arrangements are between the Australian Government and the foreign government where the non-government international stakeholder is located (as described in PSPF Guidelines Section 12.3.1 and must be in place when sharing Australian classified information with a non-government foreign entity, except in the limited circumstances described in PSPF Guidelines Section 12.3.5.1—Ad Hoc Process for Sharing with Non-Government International Stakeholders.

To enable the sharing of Australian security classified information with international non-government stakeholders, international agreements and arrangements between Australia and a foreign government may contain classified contract provisions. These provisions support the Australian Government to enter into classified contracts with non-government stakeholders in the jurisdiction of the foreign government.

International agreements that contain classified contract provisions facilitate foreign governments to undertake certain security functions for the Australian Government in relation to entities under their jurisdiction. For example, if the Australian Government establishes a classified contract with a non-government international stakeholder (involving use of Australian security classified information), the Australian Government may request under international agreements that the foreign government check the status of its facility and the personnel security clearances for that non-government international stakeholder. This provides assurance to the Australian Government that the non-government international stakeholder is capable of handling Australian Government security classified information at the appropriate security classification level.

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

Where the Australian Government engages a non-government international stakeholder on a classified contract, the foreign government is generally responsible for administering security requirements (such as providing facility and personnel security clearances) and for ensuring the security conduct of contractors within its territory under the General Security Agreement.

PSPF Release 2024 (Section 12.2) states that Australian Government security classified information or resources must not be shared with a non-government international stakeholders that are subject to extensive data collection powers or exposure to extrajudicial directions from a foreign government that conflict with Australian law.

12.3.5.1. Ad Hoc Process for Sharing with Non-Government International Stakeholders

Where no security classified information agreement or arrangement is in place that contain appropriate classified information sharing provisions, ad hoc or once off information sharing arrangements are permitted, provided written arrangements are in place that adhere to whole-of-government requirements on the protection and handling of security classified information.

These ad hoc arrangements must take risk-based approaches in sharing Australian Government security classified information and resources, where the Accountable Authority has agreed.

PSPF Release 2024 (Section 12.2.1) states that 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

  informed by a risk assessment, and
- inclusive of the protections for use and storage of security classified and caveated information and resources in accordance with the Minimum Protections and Handling Requirements and the Australian Government Security Caveat Standards.

The written ad hoc arrangements can take the form of a contract, deed or other undertaking with the non-government international stakeholder.

12.3.6 Security Clearances for Access to International Government Information and Resources

Access to security classified information and resources is restricted to those who have appropriate security clearances and a need-to-know basis for that information. This security clearance requirement also applies to foreign government information. In order to access classified foreign government information, entities are required to hold the appropriate security clearance required to access information at the corresponding Australian Government security classification.
Table 30 provides Australian Government security classification equivalencies across foreign governments.

- International agreements and arrangements can include classified information access provisions that require each party to limit access to security classified information to appropriately cleared personnel. These international agreements and arrangements can also include mutual security clearance recognition requirements.
- Entities may recognise clearances issued by Five Eyes country governments (United States, United Kingdom, New Zealand and Canada) and consequently issue corresponding Australian clearances for specific operational purposes.

The release of classified foreign government information is exempt from the *Freedom of Information Act 1982* (FOI Act). Under section 33(b) of the FOI Act, any information of a foreign government communicated in confidence to the Australian Government is an 'exempt document'. However, classified or sensitive foreign government information is not exempt from other legal processes.

Entities that are involved in legal processes where foreign government information is, or is likely to be, relevant should seek:

- legal advice on issues of relevance, disclosure and protection (including claims of public interest immunity), and
- Government permission to disclose the information, noting that disclosure may still be required under Australia's domestic legal proceedings even if permission is not obtained.

12.3.7 Release of Caveated Material under an International Agreement or Arrangement

The Australian Government Security Caveat Standard (available on need-to-know basis on GovTEAMS) outlines controls for the protection of security caveated (and compartment) information and resources used and received by the Australian Government. PSPF Guidelines (Table 24) details the common caveats and their access requirements. See PSPF Guidelines Section 9.4 for detailed information of security caveats and accountable material.

The Australian Eyes Only (AUSTEO) caveat denotes Australian Government information that is restricted to appropriately security cleared Australian citizens exclusively. Australian citizens who hold other nationalities, such as dual nationals, do not have access to information marked AUSTEO. Information sharing limitations are that information bearing the AUSTEO caveat cannot be shared with a person who is not an Australian citizen, even when an international agreement or arrangement is in place. As such, foreign access to AUSTEO caveated information is a security incident requiring CSO (or appropriate security practitioner delegate) investigation, response and reporting.

The Australian Government Access Only (AGAO) caveat denotes information that is restricted to appropriately security cleared Australian officers or representatives of foreign governments from Five Eyes countries who are on exchange, long-term posting or attachment to the National Intelligence Community (NIC) or the Department of Defence. For all other entities, information caveated AGAO is to be handled as AUSTEO and foreign access is to be treated as a security incident.

Table 30: Australian Government information and resource classification equivalencies *Note i*

Australian classification	French equivalent Note ii	US equivalent	EU equivalent	Japanese equivalent
TOP SECRET	TRÈS SECRET	TOP SECRET	TRÈS SECRET UE / EU TOP SECRET	Kimitsu 機密 Bouei Himitsu (Kimitsu) 防衛秘密(機密)
SECRET	SECRET	SECRET	SECRET UE	Gokuhi 極秘 Bouei Himitsu 防衛秘密
CONFIDENTIAL Note iii	To be handled as SECRET Note iv	CONFIDENTIAL	CONFIDENTIEL UE	Hi 秘
PROTECTED	No equivalence established Note v			
No equivalence established	No equivalence established	No equivalence established	RESTREINT UE Note vi	No equivalence established

Table Notes

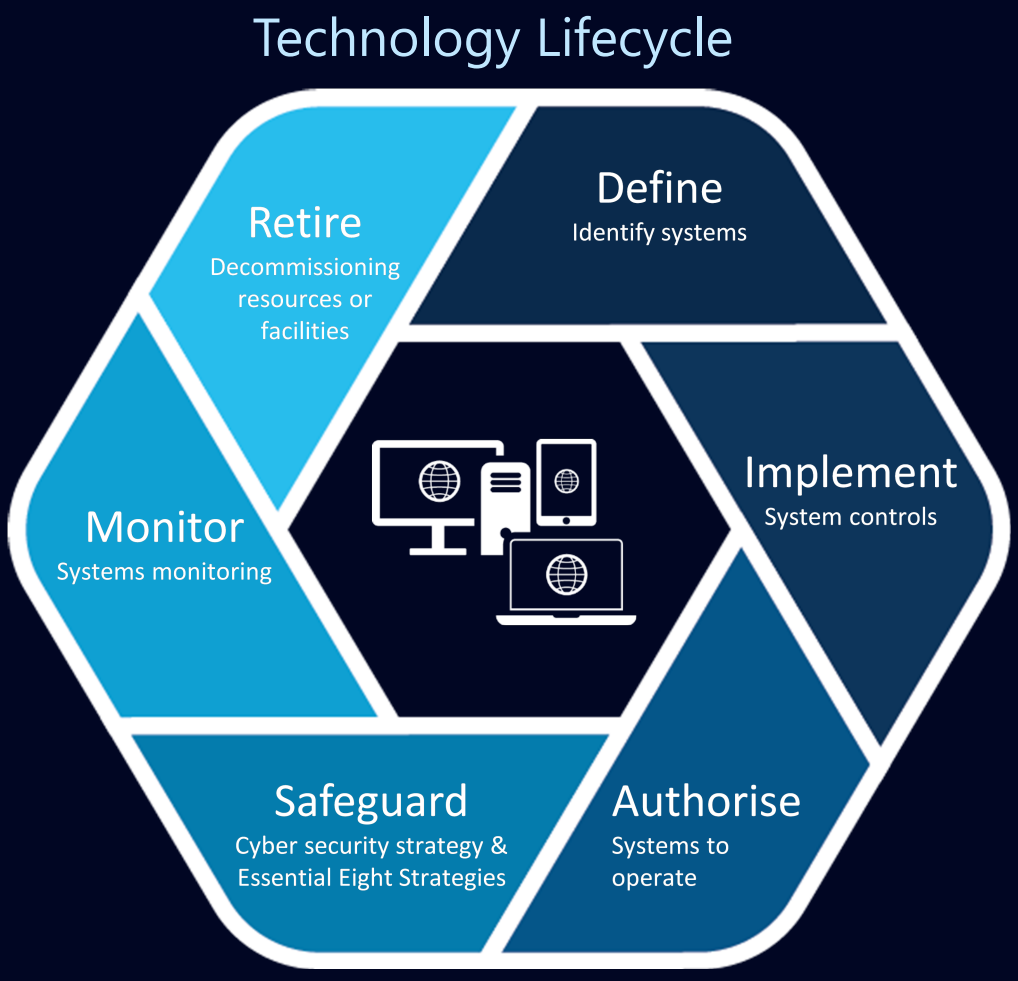
i This table identifies established equivalencies to Australian classifications only. The equivalencies do not apply between the other foreign entities listed.
ii The agreement with France also establishes equivalent protections for classified information.

iii The Australian CONFIDENTIAL classification was retired on 1 October 2020. Legacy Australian CONFIDENTIAL information is to continue to be handled by international partners as outlined in the above table. Australia will handle French CONFIDENTIEL DÉFENSE, US CONFIDENTIAL, EU CONFIDENTIEL UE, and Japanese Hi 秘 information as Australian SECRET.
iv On 1 July 2021 changes to the French classification system came into effect, removing the CONFIDENTIEL DÉFENSE classification.
v On 1 July 2021 changes to the French classification system came into effect, removing the CONFIDENTIEL DÉFENSE classification. Interim arrangements specify the handling requirements for PROTECTED information in France.
vi Implementation arrangements available from DFAT specify the handling requirements for RESTREINT UE.

Part Four

Technology

- Technology Lifecycle Management
- Cyber Security Strategies
- Cyber Security Programs



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. This includes managing the associated security risks to ensure the secure operation of each technology system the entity operates or outsources.

A technology system is defined as an entity's hardware and software used to process, store or communicate information and data, and the governance framework in which it operates.

13.1 Information Security Manual

ASD's Information Security Manual (ISM) outlines the controls to protect the entity's technology systems and data from cyber threats, using a risk management framework.

13.1.1 Cyber Security Principles

PSPF Requirement 0084 mandates that entities apply the ISM's cyber security principles during all stages of the lifecycle of each system. The phases of a technology system's lifecycle are outlined in Figure 12.

Effective implementation of the ISM cyber security principles is essential to safeguarding a technology system from cyber threats and ensuring the continuous delivery of Australian Government operations. This approach includes identifying the key security risks to each technology system and implementing appropriate and effective security controls from the ISM to manage the security risks.

The ISM's cyber security principles are grouped into four key activities:

- **Govern:** Identifying and managing security risks.
- **Protect:** Implementing security controls to reduce security risks.
- **Detect:** Detecting and understanding cyber security events to identify cyber security incidents.
- **Respond:** Responding to and recovering from cyber security incidents.

See ASD's cyber security principles for advice on assessing the level of implementation of the cyber security principles.

13.1.2 Cyber Security Controls and Guidelines

The ISM details the cyber security controls that ASD's considers to provide efficient and effective mitigations based on their suitability to achieve the security objectives for a system. Unless mandated under the PSPF, entities should consider these controls and implement those identified as necessary to address the security risks within the entity's set risk tolerances.

The guidelines provide practical guidance on how to protect technology systems, operational technology systems, applications and data from cyber threats.

PSPF Requirement 0085 mandates the ISM controls and guidelines are applied on a risk-based approach. This risk-based approach comprises the following six steps:

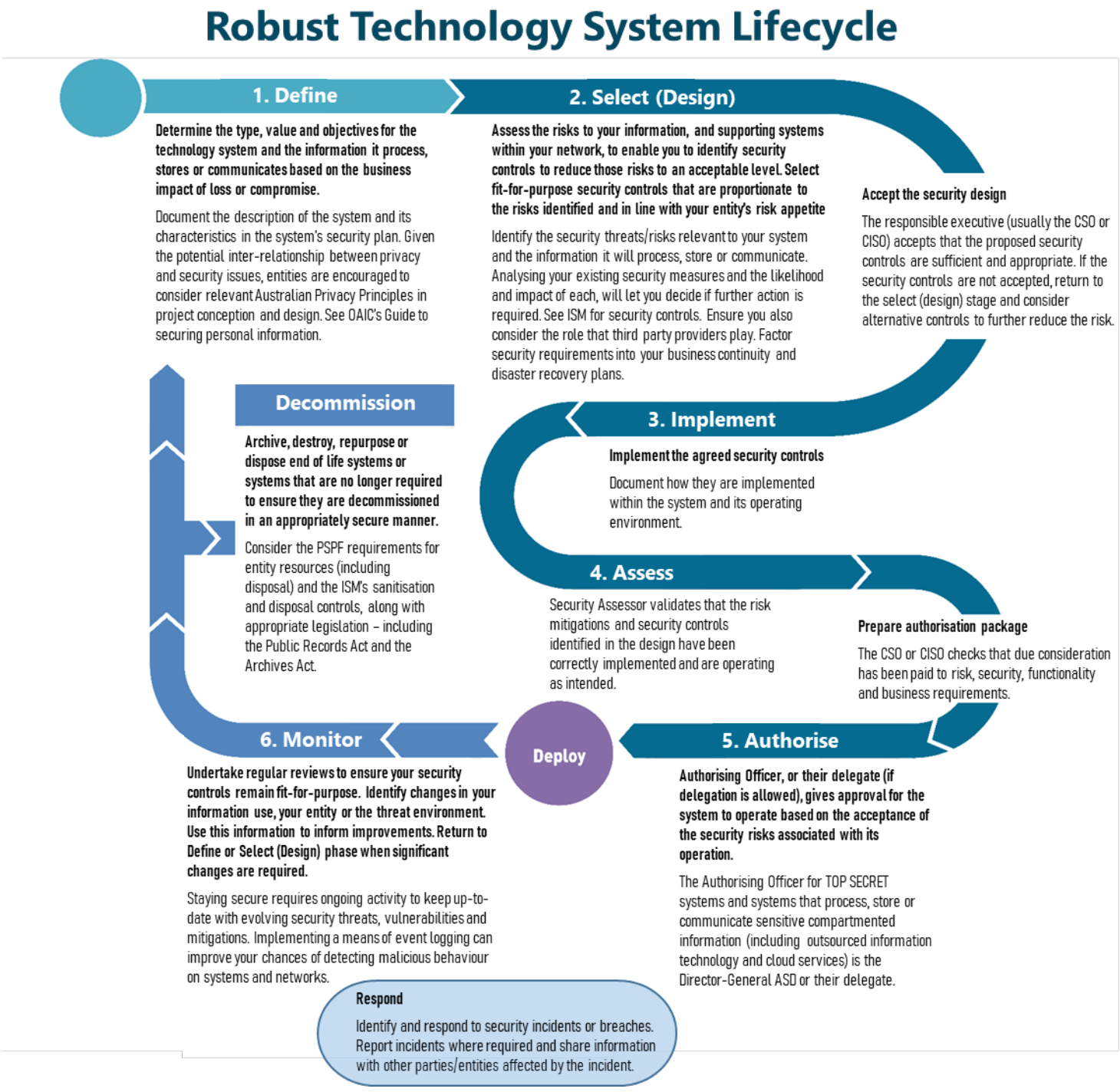
Table 31: Information Security Manual Risk-Based Approach to Cyber Security

Step	Definition
Step 1 – Define the Technology System	Determine the value of each technology system and the information and data it processes, stores and communicates, based on an assessment of the business impact of loss or compromise.
Step 2 – Select security controls	Identify the security risks to each technology system and select fit-for-purpose security controls that are proportionate to the security risks identified and consistent with the entity's agreed risk tolerances. Note that some controls are mandatory under PSPF Release 2024.
Step 3 – Implement security controls	Implement the selected security controls to reduce identified security risks to an acceptable level of residual risk and document how these security controls are implemented within the technology system and its operating environment.
Step 4 – Assess security controls	Assess the security controls for each technology system to determine whether they have been correctly implemented and are operating as intended.
Step 5 – Authorise the technology system	Authorise the technology system to operate based on the acceptance of the residual security risks associated with their operation.
Step 6 – Monitor the technology system	Monitor the security posture of each technology system to identify and respond to cyber threats and security risks while ensuring security controls remain effective and fit-for-purpose for the system's operating and threat environment. If significant or extensive adjustments are identified, it is recommended to return to the 'define the technology system' phase of the lifecycle to recommence authorisation for that technology system to operate.

See Using the Information Security Manual for further information on applying a risk-based approach to cyber security.

Figure 12 outlines the risk-based process for authorising a technology system to operate and managing security risks during all stages of the lifecycle of the system. It also notes the need to consider when to decommission (or dispose of) a system at the end of its life.

Figure 12: Robust Technology System Lifecycle



13.2 Network Documentation

Network documentation is developed to accurately depict the current state of the entity's networks 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. Finally, as network documentation could be used by malicious actors to assist in compromising networks due to the detailed nature of information it captures, it is important that it is

appropriately protected. Entities should ensure that their network documentation is suitably protected, based on the security classification or business impact level of the data.

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

See PSPF Guidelines Section 10.1 to determine whether their network documentation as an aggregated source of data could pose a significant security vulnerability to an entity's technology system and could be leveraged be by malicious actors to assist in compromising network.

13.3 Technology System Authorisation

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 decision.

PSPF Release 2024 mandates:

- PSPF Requirement 0086: 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.
- PSPF Requirement 0087: Decisions to authorise (or reauthorise) a new technology system or make changes to an existing technology system are based on the ISM's risk-based approach to cyber security.
- PSPF Requirement 0088: The technology system is authorised to the highest security classification of the information and data it will process, store or communicate.
- PSPF Requirement 0089: 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.

PSPF Release 2024 (Table 21) details the Authorising Officer and Security Assessor for each technology system:

- Security Assessor**:** reviews the system architecture, including security documentation, and assesses the implementation and effectiveness of security controls. These assessments are typically undertaken by an Infosec Registered Assessors Program (IRAP) assessor or entity personnel with the appropriate capability.
- Authorising Officer**:** reviews the authorisation package and makes an informed risk-based decision as to whether the security risks associated with the technology system's operation are acceptable or not, and grants authorisation for the system to operate. The authorisation package includes the technology system's system security plan, incident response plan, continuous monitoring plan, security assessment report, and plan of action and milestones.
    - The Authorising Officer is typically the Accountable Authority, CSO or CISO. However, this function can be delegated to another suitably senior officer where required.
    - For TOP SECRET systems and systems that process, store or communicate TOP SECRET or sensitive compartmented information and data, Director-General ASD (or their delegate) is the Authorising Officer.

See the ISM for further information on conducting security assessments and the authorisation package.

13.3.1 Technology System Reauthorisation

PSPF Requirement 0090 mandates that entities reassess each technology system's suitability to be authorised when it undergoes significant functionality or architectural change, or where the system's security environment has changed considerably.

Examples of events that may trigger additional risk management activities for a technology system include:

- changes of application in the ISM'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.

When an entity is required to reauthorisation a technology system due to one or more of the above events, the entity must follow the process detailed in the PSPF Guidelines Section 13.3 to ensure that the PSPF requirements for technology system authorisation are met.

13.3.1.1. Continued Authorisation

Entities should monitor each technology system 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 detailed in the PSPF Guidelines Section 13.3.1 warrant a full reassessment and reauthorisation of the technology system.

13.3.2 System Owners

System owners are responsible for ensuring the secure operation of their technology systems.

The entity's Authorising Officer should appoint a designated system owner to each technology system in use and must authorisation them to operate each technology system in accordance with PSPF Guidelines Section 13.3 to ensure that the PSPF requirements for technology system authorisation are met.

An entity should define the responsibilities of the system owners in accordance with the controls outlined in the ISM. These responsibilities may include the:

- determining the cyber security objectives for each technology system based on a risk assessment
- selecting appropriate cyber security controls for each technology system to achieve the desired security objectives, in accordance with the PSPF requirements, the ISM, and ASD's Essential Eight mitigation strategies (as outlined in PSPF Guidelines Section 14.2)
- implementing the selected cyber security controls and ensuring they have been implemented correctly and are operating as intended
- monitoring each technology system for associated cyber threats, risks, and appropriate controls, on an ongoing basis, and

- reporting on the security status of each technology system.

System owners may delegate the day-to-day management and operation of their technology systems to other personnel.

Recommended Approach

- Annual reporting by an entity's system owners to the entity's Authorised Officer on the security status of their technology systems can assist in maintaining awareness of the security posture of the technology systems within the entity.

13.3.3 Cyber Security Considerations for Technology Systems

Entities should actively considering a range of cyber security topics when establishing a new technology system, implementing improvements to a current system or performing maintenance of an existing system. Entities should evaluate these considerations early in the technology system lifecycle, preferably during the initial design phase of the system, to ensure they are adequately incorporated into the long-term lifecycle.

Table 32 outlines the key cyber security topics that entities should consider, in accordance with ASD's guidelines. Ongoing consideration of these topics throughout the lifecycle of a technology system is important in protecting technology systems from cyber security threats.

Table 32: Cyber Security Considerations Technology Systems

Security Considerations	Applicable PSPF Requirements, Description, PSPF and ISM Guidance
Cyber security roles	PSPF Requirement 0008 and PSPF Requirement 0011 Mandates the requirement for both the CSO and CISO roles. PSPF Guidelines: Section 2.2 and 2.3 ISM Guidance: Guidelines for Cyber Security Roles
Cyber security incidents	PSPF Requirement 0026 Early identification of a cyber security incident and timely reporting to the entity's CSO or CISO is critical to expediting containment and recovery. PSPF Guidelines: Section 3.6 ISM Guidance: Guidelines for Cyber Security Incident
Procurement and outsourcing risks	Outsourcing can be a cost-effective option for providing both managed services and cloud services, as well as potentially delivering a superior service. However, it can also affect an entity's security risk profile. For further guidance see the Information PSPF Guidelines: Section 6.1 ISM Guidance: Guidelines for Procurement and Outsourcing
Security documentation	PSPF Requirement 0008 and PSPF Requirement 0018 Mandates the creation of security plan. Preparing relevant documentation supports implementing PSPF policy and ISM guidance. PSPF Guidelines: Section 3.1 ISM Guidance: Guidelines for Security Documentation
Physical security	PSPF Release 2024 (Part Six) Outlines the physical security requirements for technology equipment and facilities. PSPF Guidelines: Section 9.3 and Section 25 ISM Guidance: Guidelines for Physical Security

Security Considerations	Applicable PSPF Requirements, Description, PSPF and ISM Guidance
Personnel security	PSPF Requirement 0024 Entities are required to ensure all personnel are provided with security awareness training. PSPF Guidelines: Section 3.5 ISM Guidance: Guidelines for Personnel Security
Access control	PSPF Requirement 0130 Entities are to control access to technology systems, networks (including remote access), infrastructure and applications. A well-structured and robust technology system allows necessary access for personnel to undertake their work while protecting security classified information and data, intellectual property and personal information. PSPF Guidelines: Section 17 ISM Guidance: Guidelines for Personnel Security
Communications infrastructure	Infrastructure security includes good cable management and security regimes that help entities maintain the integrity and availability of communications infrastructure as well as the confidentially of information and data. PSPF Guidelines: Section 13.2 ISM Guidance: Guidelines for Communications Infrastructure
Communications systems	It is important to consider other types of devices and services that are attached to a technology system. For example, telephone systems, video conferencing, internet protocol telephony and multifunctional devices. PSPF Guidelines: Section 13 ISM Guidance: Guidelines for Communications Security
Enterprise mobility	Deployment of mobile devices including smartphones, tablet and laptops, requires sound security practices for both user and device management. PSPF Guidelines: Section 9.3 ISM Guidance: Guidelines for Enterprise Mobility
Evaluated product security	As part of supply chain risk management activities it is important that entities gain assurance that products with a security function perform as claimed by vendors and provide the necessary measures to mitigate cyber threats. There are a number of methods to achieve assurance, including through formal and impartial evaluation. ASD performs limited product evaluations through the following programs: • Enterprise Mobility Evaluation Program: for enterprise mobility products used to protect security classified information and data. • High Assurance Evaluation program: for products used to protect SECRET and TOP SECRET information and data. • Australasian Information Security Evaluation Program (AISEP): for product evaluations in accordance with the Common Criteria. PSPF Guidelines: Section 6.2.2Error! Reference source not found. ISM Guidance: Guidelines for Evaluated Products
Technology equipment management	Technology equipment requires ongoing management to ensure the information and data it processes, stores or communicates remains protected in an appropriate manner. For guidance on technology system management, maintenance, repairs and sanitisation or disposal. PSPF Guidelines: Chapter 13

Security Considerations	Applicable PSPF Requirements, Description, PSPF and ISM Guidance
	ISM Guidance: Guidelines for Information Technology Equipment
Media security	Implementing sound security practices when connecting, storing, transferring, sanitising, destroying or disposing of media plays a major role in reducing cyber threats and preventing the unauthorised disclosure of security classified information and data. Media security is particularly important when decommissioning a technology system. PSPF Guidelines: Section 9.3 and section 11 ISM Guidance: Guidelines for Media
System hardening	Newer versions of operating systems often introduce improvements in security functionality over older versions. Using older versions of operating systems, especially those no longer supported by vendors, exposes entities to exploitation techniques that have since been mitigated in newer versions of operating systems. PSPF Guidelines: Section 14.2.7 ISM Guidance: Guidelines for System Hardening
System management	Secure system administration allows an entity to be resilient in the face of targeted cyber intrusions by protecting administrator workstations and accounts from compromise, as well as making adversary movement throughout a network more difficult. PSPF Guidelines: Section 14.2.4 ISM Guidance: Guidelines for System Management
Continuous system monitoring	Continuous monitoring of a technology system can assist in proactively identifying, prioritising and responding to security vulnerabilities and provide valuable information and data about exposure to cyber threats. PSPF Guidelines: Section 3.3 ISM Guidance: Guidelines for System Monitoring
Software development	It is important to implement and maintain measures to protect against software and database security vulnerabilities that may be used to undermine the integrity or availability of a technology system or its information and data. PSPF Guidelines: Section 13.4 ISM Guidance: Guidelines for Software Development
Database Systems	Hosting database servers and web servers within the same operating environment increases the likelihood of database servers being compromised by malicious actors. PSPF Guidelines: N/A ISM Guidance: Guidelines for Database Systems
Email management	PSPF Release 2024 (Section 9 – Classifications and Caveats) outlines the requirements to identify security classified information, including information and data such as emails and using an applicable protective marking. Also provides guidance for applying protective markings and, where relevant, information management markers, on emails exchanged in and between entities. PSPF Guidelines: Section 9.6 ISM Guidance: Guidelines for Email
Networking	Network management practices and procedures assist in identifying and addressing network design or configuration vulnerabilities. It is important that network documentation accurately depicts the current state of a network. PSPF Guidelines: Section **Error! Reference source not found.**

Security Considerations	Applicable PSPF Requirements, Description, PSPF and ISM Guidance
	ISM Guidance: Guidelines for Networking
Cryptography	Cryptography is primarily used to restrict access to information and data to authorised users. It provides confidentiality, integrity, authentication and nonrepudiation of information and data and actions. Encryption protects the confidentiality of information and data by making it unreadable to unauthorised users. PSPF Guidelines: N/A ISM Guidance: Guidelines for Cryptography
Gateway security	Gateway security assists in mitigating security risks by securely managing data flows between different security domains. PSPF Guidelines: Section 15.3 ISM Guidance: Guidelines for Gateways
Data transfers	Implementing formal procedures can assist in ensuring that information and data transferred between technology systems is done in a secure and verifiable manner. PSPF Guidelines: Section 9.3.3 ISM Guidance: Guidelines for Data Transfers

13.4 Applications Management

All applications require approval to be installed or used on resources that access Australian Government technology systems, information or data. The application management process ensures applications are managed from procurement decisions, deployment of the application, maintenance through to decommission.

To be effective, this process requires a combination of:

- governance procedures – that guide decisions on why this application is needed and an assessment on whether the application is safe for the entity to use and appropriately secure to have access to security classified systems, information or data, and
- application control – to ensure that only approved applications can be executed and to prevent unapproved or malicious applications (also known as malware) from running. Application control can also contribute to the identification of attempts by a threat actor to execute malicious code on a system. See PSPF Guidelines Section 14.2.5—Application Control.

13.4.1 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 approve installation of social media applications on entity mobile devices, systems or on resources that will have access to security classified information or data, need to be made on an assessment of the risk.

Assessing these risks is vital where the application is produced by vendors that are subject to extrajudicial directions from a foreign government whose laws conflict with Australian law.

The main areas of concern arise from:

- extensive data collection that social media applications typically collect extensive data as part of their business model
- exploitation of personal information posted to social media that can be exploited, including seemingly benign posts, messages, photos or videos which can be used to develop detailed profiles of individuals

- identity theft, fraud and reputation damage, and
- unreputable or untrustworthy content or disinformation present in some media applications.

These applications should only be approved for use if a legitimate business reasons exists. Legitimate business reason means a need to install or access the application on a government device to conduct business and/or achieve a work objective of an entity.

See ASD's Security tips for social media and messaging apps

13.4.1.1. 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.

PSPF Requirement 0091 mandates that entities ensure that 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.

This requirement only applies to the TikTok application and does not restrict access to TikTok through the use of a web interface (for example, accessing through a website).

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. A legitimate business reason would include:

- where the application is necessary for the carrying out of regulatory functions including compliance and enforcement functions
- where an entity requires research to be conducted or communications to be sent to assist with a work objective (for example, countering misinformation or disinformation), or
- where an entity must use the application to reach key audiences to undertake marketing or public relations activity on behalf of the entity.

PSPF Requirement 0092 mandates that the CSO or CISO 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.

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.

13.5 Legacy Information Technology Management

PSPF Release (Section 13.5) defines an Information Technology (IT) product (i.e. hardware, software, services, protocols, and/or systems) as being considered to be 'legacy' when it meets one or more criteria in both Category A and Category B below.

13.5.1 Category A

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

13.5.2 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.

All IT products will eventually become legacy over their lifespan and will introduce significant and enduring cyber security risks to an entity's technology systems.

Entities should develop a strategy to mitigate the security risks posed by legacy IT products and integrate it into their broader technology system lifecycle management approach.

An entity's strategy for mitigating legacy IT systems and products should include:

- understanding the specific cyber security risks and vulnerabilities posed by legacy IT products as they apply to an entity's technology systems
- planning for the risks associated with legacy IT products during procurement as part of procurement
- developing an accurate register of all IT products in use in an entity's technology systems,

- monitoring and maintaining the IT product register with regular reviews to ensure the register is up to date and that the IT products have adequate vendor support
- replacing legacy IT products with products that are still vendor supported
- applying temporary mitigations to legacy IT when replacement is not yet feasible

The most effective method to mitigate the risk posed by legacy IT systems is to replace it before it with IT that is still supported. PSPF Requirement 0093 mandates that entities apply ASD's Temporary Mitigations for Legacy IT to manage legacy IT products that cannot be immediately replaced. These mitigations are suitable as temporary mitigation strategies and are detailed in Table 33 below.

Table 33: Temporary Mitigations Strategies for Legacy IT Systems

Temporary Mitigation Strategy	Definition
Network segmentation and/or segregation	• Restrict exposure of legacy IT products to the internet. • Run legacy operating systems within virtual environments.
Common hardening techniques	• Do not deploy legacy operating systems in their default state. • Disable unused services (e.g. Print Spooler, fax services and Bluetooth). • Close unused network ports.
Multi-factor authentication and account hygiene	• Apply multi-factor authentication in accordance with ASD's Essential Eight mitigation strategies. See PSPF Guidelines Section 14.2.3. • Implement account hygiene practices including: o Restricting user access to legacy IT systems o Removing old and/or unused user accounts
Logging and monitoring	• Logging and monitoring of legacy IT products, where possible to a centralized logging location. • Monitor legacy IT system for information leakage from default error pages of legacy applications that may expose sensitive or security classified information.
Attack surface reduction	• Removing configuration weakness • Minimising capabilities and functionality of applications • File Type Blocking to block typically insecure file types (e.g. binary and beta file types from Microsoft Office).
System availability and access	• Shut down or close legacy IT systems and applications that are only required for specific discrete periods when not in use to prevent unauthorised access.

For further guidance from ASD, see also:

- End of Support for Microsoft Windows and Microsoft Windows Server
- Gateway Security Guidance Package: Gateway Operations and Management
- Information Security Manual

13.5.3 Legacy Information Technology Examples

The following examples are not prescriptive or comprehensive. They are provided to illustrate the reasoning an entity should employ when assessing whether a particular technology system may be considered legacy IT. Entities must refer to the technology system's characteristics as they are at the time the assessment is being made, rather than the likely future characteristics.

Examples of Legacy Technology Systems

Example 1: An entity still implements TLS v1.2, due to software deployed by vendors to enable automated transactions between the entity and clients. While implementing TLS v1.2 is not aligned with the ISM, because it is not the latest version of TLS, it is not yet out of support or end-of-life. Consequently, neither of the Category A requirements are met and the cryptographic protocol is NOT 'legacy'.

Example 2: An entity is running a telephone exchange platform, which receives no support from the original or reseller vendor (Category A). However, the entity has contracted a specialist third party support company to supply spare parts for the platform and write new code to fix bugs and add features to it. For the time being, this arrangement is cost-effective and effectively manages the risks resulting from the platform, which remains essential to the entity's business. Consequently, no criteria from Category B are met and the platform is not 'legacy'.

Example 3: An entity simply uses a mainframe for its banking, which still receives some support from the vendor and is not end-of-life. Without further information, neither of the Category A requirements are met and the mainframe is NOT 'legacy'.

Example 4: An entity uses a mainframe for its banking, which runs off AIUX-OS. This operating system is out of support from the vendor (Category A) and the mainframe cannot be upgraded to a supported version (Category B). Consequently, the mainframe platform is 'legacy'.

Example 5: An entity is using HPE 3PAR 7000 series storage as dedicated storage for a system, which is no longer covered by service or maintenance contracts from the vendor (Category A). Current support for the system is provided by some internal staff and contractors, but most existing and new staff are trained on the new corporate storage system and the necessary skill sets are diminishing due to a change in staff capabilities (Category B). Replacement spare drives, funded by a Capex project, are reducing, as drives are replaced as they fail (Category B). Consequently, the storage is 'legacy'.

Example 6: An entity still enables SSL v3 because it is obliged to provide a service to Australian citizens, some of whom cannot access the entity's online platforms using the old desktop computers they own without SSL v3. This protocol is officially obsolete (Category A). Its vulnerabilities to attacks places it above the acceptable risk threshold of the entity (Category B). Consequently, the cryptographic protocol is 'legacy'.

Example 7: An entity has built its entire business process around a bespoke piece of software which was written for specific hardware. The hardware is now end-of-life (Category A) and out of support from the vendor (Category A). It is financially impractical for the entity to build a new business process and software to move off of the hardware (Category B), the vulnerabilities of which are well above the entity's acceptable risk threshold (Category B). Consequently, the system is 'legacy'.

13.6 Technology Asset Storage

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
- data centres
- storage areas for equipment that hold, store, process or communicate official information, and
- communication and patch rooms.

See PSPF Guidelines Section 15.2.1 for detailed guidance on the Australia Government Hosting Certification Framework as it relates to PSPF Requirement 0111.

See PSPF Guidelines Section 15.2.2 for detailed guidance on the use of outsourced data centre suppliers and associated infrastructure, and the use of Digital Transformation Agency's (DTA) Data Centre Facilities Supplies Panel as mandated by PSPF Requirement 0112.

13.6.1 Technology Assets Housed in Security Zone

PSPF Requirement 0094 mandates that entities must store technology assets and their components that are classified as SECRET or below, in the appropriate Security Zone based on their aggregated security classification or business impact level.

Security Zones define restricted access areas with increasing restrictions and access controls as the Security Zones progress from Zone One to Zone Five.

See PSPF Guidelines Section 24 for detailed information on Security zones.

13.6.2 Technology Asset Housed in Layered Security Zones

Entities may be able to lower the physical security of containers required to house technology assets and their components as mandated by PSPF Requirement 0094 when the facility housing the assets 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.

This approach is known as security-in-depth, which is a multi-layered system in which security measures combine to make it difficult for an intruder or authorised personnel to gain unauthorised access to technology assets and their components.

13.7 Technology Asset 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.

PSPF Requirement 0097 mandates that entities securely dispose of technology resources in accordance with the ISM. Entities may also set additional entity-specific procedures beyond those detailed in the ISM.

Technology assets that create, send, receive or processes official Australian Government information must be disposed of in accordance with PSPF Release 2024 (Section 11), as it is considered a Commonwealth record. Section 11 includes:

- PSPF Requirement 0073 mandates that OFFICIAL and security classified information is disposed of securely in accordance with the Minimum Protections and Handling Requirements, ISM, the Records Authorities, a Normal Administrative Practice and the *Archives Act 1983*.
- PSPF Requirement 0074 mandates that security classified information is appropriately destroyed in accordance with the Minimum Protections and Handling Requirements when it has passed minimum retention requirements or reaches authorised destruction dates.

Not all official information is kept forever and disposing of it does not always mean it is 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.

Entities should remove labels and marking indicating the owner, security classification or any other marking that can associate technology assets with its prior use, to ensure it does not draw undue attention following its disposal.

13.7.1 Destruction Equipment

Destruction equipment is used to dispose of physical security classified information, including both paper-based information and technology assets, so that resultant waste particles cannot be reconstructed to enable the recovery of information.

The Security Construction and Equipment Committee (SCEC) is responsible for evaluating security equipment for their suitability for use by the Australian Government, including the evaluation of destruction equipment.

Evaluated products are assigned a security level (SL) rating numbered 1 to 4. Approved items are listed in the SCEC Security Equipment Evaluated Product List (available to government personnel on GovTEAMS).

For further guidance see:

- PSPF Guidelines Section 25.1 for detailed information on SL ratings as they apply to destruction equipment
- PSPF Guidelines Table 57 provides a summary of the destruction equipment that is tested by SCEC and appears in the SEEPL and Security Equipment Guides, and
- PSPF Guidelines Section 11.1 for detailed guidance on the methods for secure destruction of information in physical form, including the destruction of security classified information.

13.7.2 Disposal of Physical Resources

Entities may need to dispose of entity physical resources due to advances in technology, the end of the usable life of the physical resource, and downsizing and changes in business requirements. Entities should dispose of physical resources securely.

Prior to decommissioning and disposal of physical resources such as security containers, cabinets, vaults, strongrooms and secure rooms, entities should:

- reset combination locks (electronic and mechanical) to factory settings, and
- visually inspect and remove all contents from these physical assets.

14 Cyber Security Strategies

14.1 Cyber Security Strategy

A cyber security strategy articulates the entity's plans, objectives, and priorities for cyber security uplift to manage cyber security risks posed to the technology systems and resources of an entity in accordance with the ISM.

The PSPF Guidelines Section 3.1—Security Planning details how an entity should adopt a security planning approach, including how to establish a robust security plan. The same guidance should be applied to establishing a cyber security strategy.

The PSPF Guidelines Section 13—Technology Lifecycle Management outlines the technology lifecycle management approach which aims to secure an entity's information technology and operational technology systems (technology systems) by providing detailed guidance on how an entity should apply the ISM's cyber security principles, as mandated by PSPF Release 2024, and how to implement the risk-based approach to cyber security controls.

An entity's cyber security strategy should articulate how cyber security risks are managed in the entity, how an entity plans to implement the technology lifecycle management approach, and how the entity plans to address the requirements outlined in the PSPF in accordance with the ISM and ASD's Essential Eight mitigations strategies (as outlined in PSPF Guidelines Section 14.2). Critically, it aligns these strategies with the entity's strategic goals, priorities, and objectives.

The first step in developing a mature cyber security strategy is for an entity to understand and outline:

- what the entity needs to protect (via a risk assessment) being the technology systems and resources in use by the entity.
- what it needs to protect against (via threat assessment), being specific vulnerabilities to the technology systems and resources, and more broadly, the current cyber threat landscape.
- how cyber security risks will be managed within the entity, including the specific rules and information security controls in line with the ISM and ASD's Essential Eight mitigations strategies.

The cyber security strategy reflects the entity's cyber security requirements and mitigation strategies appropriate to the current threat landscape, the risks to its technology systems and resources, and the entity's risk tolerances. The process for developing a cyber security strategy is divided into several key steps, outlined in Table 34.

Table 34: Cyber Security Strategy Development Process

Step	Definition
Define existing baseline	Outlines the technology systems and resources that an entity needs to protect, and what it needs to protect against. This includes detailing the entity's current cyber security posture and maturity by reviewing the: • existing technology systems and resources in use by the entity • environment in which the entity operates including the threats, risks, and vulnerabilities • existing cyber security policies and controls implemented by the entity
Design	Details the entity's cyber security goals and strategic objectives and how cyber security risks with be managed by:

Step	Definition
	• defining the cyber security goals • detailing the entity's tolerance to security risks • detailing the entity's current capability to manage cyber security risks • outlining how the goals and strategic objective address the threats, risks, and vulnerabilities posed to the entity, and • prioritising and communicating how the strategy supports the broader business objectives as reflected in the entity's corporate plan.
Implement	Entities should implement their cyber security strategy by prioritising the goals and strategic objectives outlined during the design phase.
Monitor	Entities are to continually monitor their cyber security strategy to proactively identify, prioritise and respond to cyber security risks.
Review	Entities are to review their cyber security strategy to ensure it addresses the contemporary cyber security threat landscape. It is recommended the cyber security plan also be reviewed when there are significant shifts in the entity's risk, risk tolerance or operating environment. Entities should: • continually improve practices for cyber security risk management. • review emerging cyber security threats and broadly review changes to the cyber threat landscape to ensure that the cyber security plan stays fit-for-purpose and adequately respond to risks, and • review and adjust the cyber security strategy to ensure the goals and strategic objectives match with changes to the entity's organisational and management priorities.

Regardless of an entity's functions or cyber security concerns, the central messages for managing cyber security risks are:

- Cyber security is everyone's responsibility and risk management is the business of all personnel (including contractors) in the entity, supported by cyber security awareness training.
- Cyber security is a business enabler that informs decision-making, is part of day-to-day business and is embedded into an entity's business processes.
- Cyber security management is logical, systematic and transparent and is part of the enterprise risk management process.
- Cyber security processes identify changes in the threat environment and allow for adjustments to maintain acceptable levels of risk, balancing operational and cyber security needs.

When developing or reviewing the cyber security strategy entities are encouraged to seek advice and technical assistance from specialist entities such as:

- ASIO for threat assessments
- ASD for IT, technology systems, cyber security and certified cloud services advice, and
- subject-matter experts.

For guidance on cyber security strategies, see ASD's Strategies to Mitigate Cyber Security Incidents, Essential Eight Maturity Model, Guidelines for Security Documentation and Secure-by-Design Foundations.

14.2 Essential Eight Strategies

PSPF Requirement 0099 to PSPF Requirement 0106 mandates that entities implement the Essential Eight mitigation strategies from ASD's Strategies to Mitigate Cyber Security Incidents to Maturity Level Two under the Essential Eight Maturity Model.

The mitigation strategies that constitute the Essential Eight are:

- patch applications
- patch operating systems
- multi-factor authentication
- restrict administrative privileges
- application control
- restrict Microsoft Office macro settings
- user application hardening, and
- regular backups.

Recommended Approach

- Implement a mitigation strategy that first implements for high risk users and computers with access to important (security classified or high-availability) data for internet-facing services and systems before implementing more broadly.

14.2.1 Patch Applications

Applying patches to applications of technology systems assists in preventing the execution of malicious code and limiting the extent of cyber security incidents.

Patches for security vulnerabilities come in many forms. These include:

- Fixes that can be applied to pre-existing application versions.
- Fixes incorporated into new applications that require replacing pre-existing versions.
- Fixes that require overwriting of the firmware on network devices.

Once a patch for a vulnerability is released by a vendor, it should be patched in a timeframe commensurate with the severity of the vulnerability and the entity's exposure to it.

Entities should use vulnerability scanners to assist in gathering information on missing patches in their environment. In cases where vulnerability scanners can't be used, organisations should refer to vendor documentation on how to conduct manual audits.

Entities should prioritise patching key business applications that routinely interact with untrusted content from the internet. Key business applications can include:

Table 35: Key Business Applications for Patching

Application	Example Products
Office productivity suites	• Microsoft Office • Microsoft Excel
PDF Readers	• Adobe Acrobat
Web Browsers	• Microsoft Edge

	• Mozilla Firefox • Google Chrome
Web Browser Plugins	• Adobe Acrobat • Ad Blockers
Email Clients	• Microsoft Outlook
Security Products	• Host-based Intrusion Protection Systems (HIPS) • Endpoint Detection and Response software • Software Firewalls (e.g. Symantec, Sophos, Azure Firewall) • Anti-Virus Software • Device access control
Software Platforms	• Oracle Java Platform • Microsoft .NET Framework • Microsoft PowerShell

Patches may not be available for older versions of applications, for example, those no longer supported by vendors. If there are no patches available, temporary workarounds may provide an effective protection. These workarounds may be published in conjunction with, or soon after, security vulnerability announcements. Temporary workarounds may include:

- disabling the vulnerable functionality within the application
- restricting or blocking access to the vulnerable service using firewalls or other access controls.

When a patch is not available for a security vulnerability, and no temporary workaround has been provided, it is recommended that entities reduce access to the security vulnerability through alternative means by:

- disabling the functionality associated with the security vulnerability
- asking the vendor for an alternative method of managing the security vulnerability
- moving to a different product with a more responsive vendor
- engaging a software developer to resolve the security vulnerability.

See ASD's Assessing Security Vulnerabilities and Applying Patches for details of timeframes and prioritised order for applying patches. This includes applying patches for 'extreme risk' vulnerabilities within 48 hours. Entities should contact ASD for assistance if a patch is not available for an application that may expose the Australian Government to high-risk vulnerabilities.

Recommended Approaches

- ✔ Monitor relevant sources for information about new security vulnerabilities and associated patches for applications and operating systems.
- ✔ Implement a centralised and managed approach to patching operating systems and applications (where possible), including by regularly scanning for missing patches.
- ✔ Confirm that patches have been installed, applied successfully and remain in place.

See ASD's Assessing Security Vulnerabilities and Applying Patches and Strategies to Mitigate Cyber Security Incidents for guidance on patching applications.

14.2.2 Patch Operating Systems

Applying patches to operating systems of workstations, servers and network devices assists in limiting the extent of cyber security incidents.

The recommended guidance for applying patches to operating systems mirrors the guidance for patching applications as described in PSPF Guidelines Section 14.2.1—Patch Applications. Entities should:

- apply patches in a timeframe commensurate with the severity of the vulnerability and the entity's exposure to it. Operating systems with 'extreme risk' vulnerabilities should be patched within 48 hours,
- use vulnerability scanners to assist in gathering information on missing patches in their environment,
- employ temporary workarounds where security patches may not be available for older versions or for systems which are no longer supported by vendors, and
- reduce access to the security vulnerability where no patch is available and no temporary workaround has been provided.

Entities should patch operating systems in a priority order, particularly systems that routinely interact with untrusted content from the internet. The recommended order is to patch the operating systems of:

- internet-facing network devices
- internet-facing servers
- non-internet-facing network devices
- non-internet-facing servers, and
- workstations.

See ASD's Assessing Security Vulnerabilities and Applying Patches for details of timeframes and prioritised order for applying patches. This includes applying patches for 'extreme risk' vulnerabilities within 48 hours. Entities should contact ASD for assistance if a patch is not available for an operating system that may expose the Australian Government to high-risk vulnerabilities.

14.2.3 Multi-Factor Authentication

Multi-factor authentication is the process of verifying a user's identity for access to an entity's technology systems and online services to prevent an adversary from accessing security classified data.

Multi-factor authentication requires two or more authentication factors. These factors must come from two or more of the following authentication factory categories.

Table 36: Multi-factor Authentication Factors

Authentication Factor Category	Examples
Something the claimant knows	• Personal identification number (PIN) • Password
Something the claimant has	• Security key (e.g. Yubikey) • Physical hardware token (e.g. Token2) • Software soft token (e.g. Microsoft Authenticator App) • Smartcard
Something the claimant is	• Fingerprint • Facial recognition • Iris scan

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.

To manage access to their technology systems, entities should implement user identification, authentication and authorisation practices. The ISM provides technical guidance on security controls for mitigating the risks associated with privileged access to systems.

To restrict administrative privileges:

- identify tasks which require administrative privileges to be performed
- validate which staff members are required and authorised to carry out those tasks as part of their duties
- create separate attributable accounts for staff members with administrative privileges, ensuring that their accounts have the least amount of privileges needed to undertake their duties, and
- revalidate staff members' requirements to have a privileged account on a frequent and regular basis, or when they change duties, leave the organisation or are involved in a cybersecurity incident.

Entities should prevent privileged accounts from accessing the internet, unless explicitly required for the management of cloud services.

14.2.5 Application Control

Application control ensures that only approved applications can be executed to prevent unapproved or malicious applications (also known as malware) from running. Application control can also contribute to the identification of attempts by a threat actor to execute malicious code on a system. Commonly abused applications include:

- Executables (.exe files)
- Software libraries (DLLs)
- Scripts (PowerShell, HTML Applications)
- Application installers
- Compiled HTML, and
- Control panel applets.

To implement application control, entities should:

- identify approved applications
- develop application control rules to ensure only approved applications are allowed to execute
- maintain the application control rules using a change management and review program,
- validate application control rules on a frequent basis, and
- ensure that both unprivileged and privileged users cannot temporarily or permanently disable, bypass or be exempt from application control.

Entities should ensure that both unprivileged and privileged users cannot temporarily or permanently disable, bypass or be exempt from application control.

See ASD's Implementing Application Control and the application control section of Strategies to Mitigate Cyber Security Incidents for detailed guidance on implementing application control on technology systems.

14.2.6 Restrict Microsoft Office Macro Settings

To protect themselves against malicious macros, entities should disable or secure their use of Microsoft Office macros for all users that don't have a valid business requirement for their use.

Additionally, entities should disable support for trusted documents and trusted locations.

Where a valid business requirement to use macros exists, entities should:

- use macros digitally signed by trusted publishers
- use macros from trusted locations are enabled, and
- decide which macros to enable on a case-by-case basis (with additional security measures).

Recommended Approaches

- Implement an application control solution to mitigate malicious macros running unapproved applications.
- Prevent users from changing macro security settings within Microsoft Office applications.

14.2.7 User Application Hardening

Entities should consider the vendor's security record when selecting applications and use the latest versions of applications where possible and configure the applications to operate in the most secure manner.

14.2.8 Regular Backups

Regular backups assist in recovering and maintaining operations in the event of a cyber incident.

Entities should:

- ensure all important data, software and configuration settings for software, network devices and other IT equipment are captured
- ensure backups are protected from unauthorised access, modification, corruption and deletion
- determine the retention period for backups in accordance with business continuity planning
- perform backups in a coordinated manner across the entity, and
- ensure regular testing of system restoration processes as part of disaster recovery exercises.

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.

Entities should conduct an assessment of the key risks and threats to their entity and determined which remaining mitigation strategies are most important to their entity. The Strategies to Mitigate Cyber Security Incidents provides advice on prioritisation of these remaining mitigations strategies, and entities should implement the identified mitigation strategies until an acceptable level of residual risk is achieved.

PSPF Requirement 0107 further mandates that entities consider the remaining Essential Eight Strategies and implement those required to achieve an acceptable level of residual risk for 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.

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 ISM and Strategies to Mitigate Cyber Security Incidents in their annual report on security to their minister and the Department of Home Affairs.

14.4 Mark Inbound Emails from External Organisations

As part of an entity's email security awareness activities, they may elect to mark inbound emails originating from external organisation with non-government (gov.au domain) email addresses with a warning notice, to encourage recipients to exercise additional caution when clicking links or attachments associated with the email.

The notice should be:

- at the top of the email, and
- in the form of a banner to ensure visibility

An example notice is below:

> CAUTION: This email originated from outside the organisation from a non-gov.au email address. Do not click links or open attachments unless you recognise the sender and know the content is safe.

See ASD's Malicious Email Mitigation Strategies for further guidance and PSPF Guidelines Section 9.6—Email Protective Marking Standard.

15 Cyber Security Programs

15.1 Whole-of-government Cyber Security Service

PSPF Requirement 0108 mandates that entities employ a Protective Domain Name System (PDNS) service or other security mechanisms to prevent connections to and from known malicious endpoints

PDNS services automatically check incoming and outgoing network traffic against a block-list of high-risk websites and email servers, derived from cyber threat intelligence, to help prevent accidental access to harmful websites to prevent the theft of sensitive or security classified data.

The Australian Protective Domain Name Service (AUPDNS), is a free opt-in service available to all Federal, State and Territory government entities. Information from AUPDNS also assists ASD build a comprehensive national cyber threat picture, which is shared with ASD partners.

If an entity elects not to deploy a PDNS and instead relies on other equivalent security mechanisms, they should ensure that the system is configured to generate equivalent logging and telemetry data.

To sign up to the AUPDNS service please contact ASD's AUPDNS Customer Support via acscaupdns.support@defence.gov.au.

For information how to become an ASD partner, see ASD's Cyber Security Partnership.

Recommended Approach

- Entities should be aware that the use of an upstream PDNS resolver service could impair security features, such as web proxies, mail relays, sandbox and malware analysis platforms, and SIEM tools, and should assess and evaluate to ensure their security platforms are functional correctly.

15.2 Secure Cloud Strategy

PSPF Requirement 0109 mandates that entities use cloud service providers that have completed an IRAP assessment against the current version of ASD's ISM with the previous 24 months.

The Department of Home Affairs' Secure Cloud Strategy and ASD's suite of cloud security publications provides guidance on adopting cloud computing and cloud services. At its core, cloud computing involves outsourcing a part, or all, of an entity's technology 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

To ensure cloud systems have achieved the desired security baseline, these systems need to be assessed to gain assurance they meet the security requirements and risk tolerance of the organisations. This assessment should be performed by an IRAP assessor.

PSPF Requirement 0109 mandates that entities consider the recommendations and findings from the IRAP assessment and implement them on a risk-based approach.

PSPF Release 2024 (Table 21) allows the security assessments of SECRET and below systems can be undertaken by an entity's own assessors or IRAP Assessors. However it is best practice, and strongly recommended, to engage an IRAP Assessor when performing a security assessment. For commercial or government gateways, and outsourced cloud service providers and their cloud services, security assessments must be undertaken by an IRAP Assessor. In all cases, assessors should hold an appropriate security clearance and have an appropriate level of experience and understanding of the type of system they are assessing.

ASD's IRAP Consumer Guide provides advice on:

- how to engage an IRAP Assessor
- how to prepare for an IRAP assessment
- understanding the assessment process, and
- how to best use the information provided in the IRAP assessment report.

See PSPF Guidelines Section 13.3 for guidance on Technology System Authorisation and ASD's Blueprint for Secure Cloud and Cloud Assessment and Authorisation.

15.2.1 Australian Government Hosting Certification Framework

PSPF Requirement 0111 mandates that entities must ensure the secure hosting of security classified government information and data of OFFICIAL: Sensitive and PROTECTED that is processed, stored or communicated via an outsourced managed service provider or cloud service provider that has their services and associated infrastructure certified through the use of the Department of Home Affairs' Australia Government Hosting Certification Framework (HCF).

Entities must ensure that personnel of a particular outsourced managed service provider or cloud service provider who access security classified information and data have an appropriate Australian Government security clearance, briefings and a need-to-know commensurate with the security classification of the information and data being stored, processed and transmitted in their cloud services when considering the suitability of their services.

Entities seeking to procure cloud services should also self-assess cloud service providers and cloud services using the risk-based approach to cyber security outlined in the ISM, in accordance with Secure Cloud Strategy.

See HCF's list of Certified Service Providers and ASD's Guidelines for Procurement and Outsourcing.

Recommended Approach

- Entities are strongly recommended to use ASD's Anatomy of a Cloud Assessment and Authorisation for guidance when performing a security assessment to determine the suitability of a particular cloud service provider and its cloud services.

15.2.2 Data Centres

Entities that are considering the use of outsourced data centre suppliers and associated infrastructure for hosting of security classified information and data, a whole-of-government system, or system rated at the classification level of PROTECTED, must procure services from certified suppliers in accordance with the Australian Government Hosting Certification Framework.

A list of Certified Service Providers is managed by the Australian Government Hosting Certification Framework.

PSPF Requirement 0112 mandates that when entities intend to buy data centre space and services that they use the Digital Transformation Agency's (DTA) Data Centre Facilities Supplies Panel. The DTA's 'BuyICT Portal' leverages the Data Centre Facilities Supplies Panel for buying certified data centre space and services.

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

It is not encouraged that entities use foreign-owned managed service providers or cloud service providers that have not been certified under the Australia Government Hosting Certification Framework. If required,

PSPF Release 2024 Chapter 6 outlines requirements for managing security risks associated with any procurement, including the potential security risks associated with foreign involvement.

See ASD's Guidelines for Procurement and Outsourcing, Cloud Assessment and Authorisation and Identifying Cyber Supply Chain Risks.

15.3 Internet Gateway Policy

A gateway is a data flow control mechanism that securely manages data flows between connected technology systems from different security domains. The Department of Home Affairs' Gateways Policy, as part of the Resilient Digital Infrastructure Framework (RDIF), details security protections and capabilities between security domains for Australian Government gateways and the boundary between the internet and government networks.

PSPF Requirement 0113 mandates that entities must protect their internet-connected technology systems, and the information and data they process, store or communicate, by implementing a gateway consistent with the Department of Home Affairs' Gateways Policy, and the Internet Security Manual's Guidelines for Gateways which provides general guidance on gateways and assists entities in making informed risk-based decisions when consuming gateway services.

15.4 Vulnerability Disclosure Program

PSPF Requirement 0115 mandates that entities establish a vulnerability disclosure program and supporting processes and procedures to receive, verify, resolve and report on vulnerabilities disclosed by both internal and external sources. 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 VDP, 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.

A VDP should include processes and procedures covering:

- the purpose of the VDP
- types of security research that are and are not allowed
- how to report any vulnerabilities
- actions, and associated timeframes, upon notification of vulnerabilities
- expectations regarding the public disclosure of vulnerabilities, and
- any recognition or reward for finders of vulnerabilities.

See ISM's Guidelines for Software Development | Cyber.gov.au for guidance on the creation and maintenance of VDPs.

Part Five

Personnel

Pre-Employment Eligibility

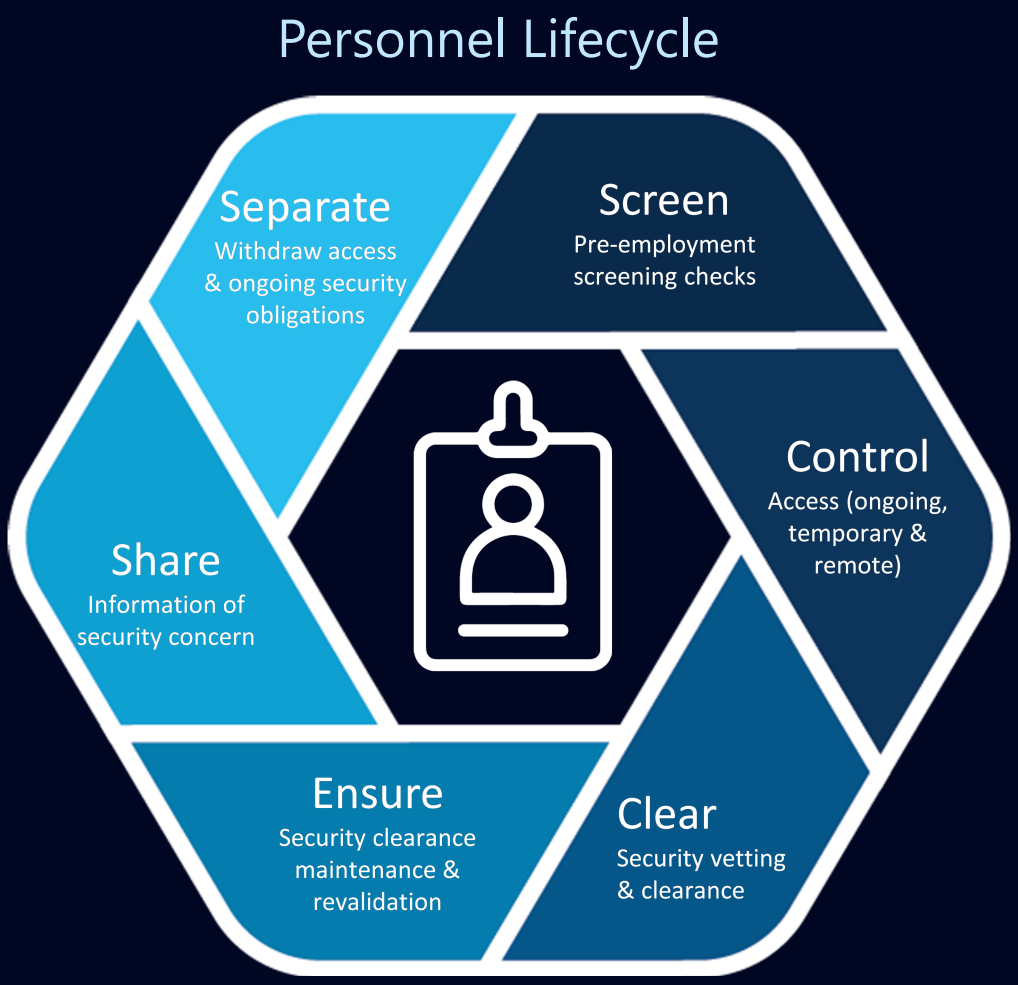
Access to Resources

Security Vetting Process

High Office Holders and their Support Staff

Maintenance and Ongoing Assessment

Separation



16 Pre-Employment Eligibility

16.1 Pre-Employment Screening

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

Completing screening prior to engagement is particularly important for positions that have been identified as requiring a security clearance. As stated in PSPF Release 2024 (Section 16.1), 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.

Entities should obtain informed consent from all personnel to collect, use and disclose personal information (including sensitive information) for the purposes of assessing and reviewing their eligibility and suitability for employment.

As part of the pre-employment screening, entities should:

- obtain informed consent from all personnel to collect, use and disclose personal information (including sensitive information)
- include a privacy statement in their recruitment and pre-employment paperwork detailing how personal information (including sensitive information) will be collected, used and disclosed, and obtain consent from all personnel to allow the entity to:
    - collect personal information, including sensitive information, from other entities or private organisations
    - disclose personal information, including sensitive information, with other entities when determining initial or continuing suitability to access official resources
    - use personal information, including sensitive information, to determine a person's ongoing suitability to access Australian Government resources, and
    - transfer information to another entity when personnel transfer.

As part of the pre-employment screening, entities are also encouraged to obtain both:

- a statutory declaration stating all information provided is truthful and complete, and
- a signed agreement to confirm their undertaking to safeguard Australian Government resources including reference to compliance with relevant legislation and policies.

In addition to secrecy provisions under the *Criminal Code Act 1995*, entities are encouraged to advise all personnel of any entity-specific legislative requirements. Entities will also need to consider any and all privacy obligations under the Australian Privacy Principles when receiving and using the information provided during pre-employment screening.

Entities should establish procedures and practices to appropriately handle and manage this information, including clear governance structures for decision-making and consultation to determine if there are identified security risks and what appropriate actions may be required. This is particularly important if receiving this information from an Authorised Vetting Agency that has been identified through a vetting process.

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.

Pre-employment screening checks are conducted after the conclusion of the merit selection process and prior to an offer of employment or contract. 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.

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.

16.1.1.1. Identity Checks

PSPF Requirement 0117 mandates that entities conduct a pre-employment screening identity for all personnel, to verify identity to at least Level 3 (High) of Assurance of the National Identity Proofing Guidelines 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.

PSPF Requirement 0118 mandates that biographic information in identity documents is verified to ensure the information matches the original record.

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 Document Verification Service 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.

16.1.1.2. Eligibility Check

PSPF Requirement 0119 mandates that entities conduct eligibility checks for all personnel, as part of the pre-employment screening, to confirm their eligibility to work in Australia and for the Australian Government. 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.

16.1.1.3. Additional Recommended Pre-Employment Screening Checks

The following recommended pre-employment checks may assist entities to further assess a person's suitability, in accordance. Pre-employment screening is recommended to align with Australian Standard AS 4811-2022-Employment Screening.

Table 37: Additional Recommended Pre-Employment Screening Checks

Check	Description
Employment history check (integrity and reliability)	• An employment history check identifies whether there are unexplained gaps or anomalies in employment. A person might not disclose periods of employment if they have had their employment terminated or anticipate an adverse referee report. A history of short periods of employment may indicate poor reliability. • Employment history information may be available from human resources areas of large employers. Alternatively, referees checks or other previous employers may provide corroborating evidence. • Employment history check for a period of at least 5 years, where applicable, is recommended for all new personnel.

Check	Description
Residential history check (integrity and reliability)	• A residential history check helps to substantiate the person's identity in the community. All personnel need to provide supporting evidence of their current permanent residential address. • Residential history check for a period of at least 5 years is recommended for all new personnel. If the person is unable to provide supporting documents to explain periods or residency, entities should make an assessment of whether the person's explanation is reasonable.
Referee check (integrity and reliability)	• A referee check helps entities engage people of the appropriate quality, suitability and integrity. • A referee check may address: o any substantiated complaints about the person's behaviour o information about any action, investigation or inquiry concerning the person's character, competence or conduct, and o any security related factors that might reflect on the person's integrity and reliability. • Professional referee checks are recommended to cover a period of at least the last 3 months.
National Police check (integrity and reliability)	• A national Police check, commonly referred to as a criminal history or police records check, involves processing an individual's biographic details (such as name and date of birth) to determine if the name of that individual matches any others who may have previous criminal convictions. • It is important that entities conducting a national police check are clear about what convictions would preclude a person from employment. The Spent Convictions Scheme outlined in Part VIIC of the *Crimes Act 1914*, requires that entities request a 'no exclusion' national Police check, unless the entity is covered by an exclusion under the Act. • A Commonwealth 'no exclusion' national police check provides a record of Commonwealth convictions for the preceding 10 years, or until there is a gap of 10 years between convictions, whichever is the longer. However, convictions reported by each state or territory will depend on their relevant spent convictions schemes. • See the Australian Federal Police (AFP) website National Police Checks and the Office of the Australian Information Commissioner Spent Conviction Scheme Fact Sheet.
Credit history check (integrity and reliability)	• A credit history check establishes whether the person has a history of financial defaults, is in a difficult financial situation, or if there are concerns about the person's finances. • A credit history check may be requested from an accredited financial credit check organisation. A number of private organisations can provide credit history checks on a fee-for-service basis. • Checking a person's credit history is recommended.
Qualification check	• A qualification check verifies a person's qualifications with the issuing authority. • Entities are recommended to verify declared academic qualifications with the issuing authorities, including universities, technical colleges or schools, as well as any professional associations or memberships that are required.
Conflict-of-interest declaration check	• A conflict-of-interest declaration identifies conflicts, real or perceived, between a person's employment and their private, professional or business interests that could improperly influence the performance of their official duties and thus their ability to safeguard Australian Government information or resources. • A conflict can be brought by (and not limited to) financial particulars, secondary employment and associations. • Developing a conflict-of-interest policy to guides staff on what could be perceived as a conflict of interest and when and how to report a conflict is recommended. • Based on their risk assessment, entities are encouraged to consider whether all personnel, not just contractors, complete a conflict-of-interest declaration. For information, see the Australian Public Service Commission (APSC) advice on Declarations of interest.

Check	Description
Entity-specific checks	• Entities should identify the checks needed to mitigate additional entity personnel security risks where not addressed by the recommended minimum pre-employment screening checks. • Additional screening checks are entity-specific and are separate from the security clearance process. o Some examples of entity-specific checks include drug and alcohol testing, detailed financial probity checks and psychological assessments. For advice, see the APSC publication Conditions of engagement. • Entities are recommended to seek separate advice from the APSC, the Australian Human Rights Commission or independent legal advice about the suitability and use of any proposed entity-specific checks.

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.

17 Access to Resources

The need-to-know principle applies to all security classified information, resources and activities. 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. See PSPF Guidelines Section 12.1 for further information on the Need-to-Know Principle.

'Resources' is the collective term for applications/technology systems/mobile devices that process, store or communicate official and security classified information/data, physical/tangible assets, equipment, facilities, buildings and other spaces/places, elements of infrastructure and intangible assets such as data centres.

17.1 Temporary Access to Resources

Temporary (rather than ongoing) access to security 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.[14] Temporary access to SECRET information requires an existing Baseline security clearance and TOP SECRET information requires an existing Negative Vetting 1 security clearance.

Temporary access to security classified information is split into two types outlined in Table 38.

The type of temporary access can be changed from short-term 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.

Table 38: Temporary Resource Access Types

Access Type	Definition
Short Term Access	Where the person does not hold a clearance at the appropriate level but has a valid need-to-know and requires access to relevant information and the risks can be mitigated. 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
Provisional Access	Where the person has commenced a clearance process by providing the relevant details for assessment by an Authorised Vetting Agency.

PSPF Requirement 0062 mandates the following minimum protections to safeguard classified resources that are accessed on a temporary basis. Entities must:

- limit the duration of access to security classified information
- supervise all temporary access, and

[14] PSPF Release 2024 states Temporary access to SECRET information requires an existing Baseline security clearance. This is incorrect, and will be amended in PSPF Release 2025.

- ensure that personnel have an existing Negative Vetting 1 security clearance for short-term or provisional access to TOP SECRET information.

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

Recommended Approaches

- Where an entity intends to grant temporary access to security classified information from another entity or third party, they should consult the other entity or party and obtain agreement for temporary access to their security classified information.
- Obtain a confidentiality or non-disclosure agreement to protect security classified information.

17.1.1 Temporary Access Risk Assessment

PSPF Requirement 0122 mandates that entities conduct a risk assessment to determine whether to allow temporary access to classified information.

As mandated in PSPF Release 2024 (Section 17.1.1), 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 Authorised Vetting Agency that the person has no identified concerns, or a clearance that has been cancelled or denied
- potential 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.

17.1.2 Supervise Temporary Access

PSPF Requirement 0123 mandates that entities must supervise all temporary access to security classified information, resources and activities.

Supervision may 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)

- monitoring and audit logging (and related audit trails) are key measures to control access to technology systems and the information held on those systems.

17.1.3 Limit Duration of Temporary Access

PSPF Requirement 0124 mandates that entities must limit the duration of access to security classified information.

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 for all entities.

- 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), where 12-months refers to the preceding 12-months from the date the short-term access would be granted, and
- Provisional access —an individual can be granted access until a security clearance is granted or denied. Provisional access should be reviewed annually to ensure the clearance subject remains suitable to hold provisional access.

17.2 Ongoing Access to Resources

Access to security classified information necessitates a high level of assurance of a person's integrity. This is due to the potential harm associated with compromise of that information.

In addition to requiring a need-to-know basis, ongoing access to security classified information is limited to personnel with the necessary security clearance. Table 39 details the minimum security clearance levels for ongoing access to each information classification level.

PSPF Requirement 0132 mandates that personnel requiring ongoing access to security classified information or resources are security cleared to the appropriate level, and although OFFICIAL: Sensitive is designated as a security classification, personnel are not required to hold a security clearance to access information at this level. They only require an appropriate employment screening check.

Table 39: Minimum Security Clearance Levels for Ongoing Access to Information

	Security classified information			
OFFICIAL	OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
Security clearance not required. (For entity personnel, employment screening is sufficient).	Security clearance not required. (For entity personnel, employment screening is sufficient).	Baseline security clearance or above is required.	Negative Vetting 1 security clearance or above is required.	Negative Vetting 2 security clearance or above is required.

17.2.1 Access to Caveated Information

Security caveats are a warning that the information has special protections and handling requirements in addition to those indicated by the security classification.

PSPF Requirement 0133 mandates that personnel requiring access to caveated information must meet all clearance and suitability requirements imposed by the originator and caveat controlling authority.

Access to caveated information that involves a codeword requires a briefing and a security clearance. Security caveats, and their access requirements, are outlined in the PSPF Guidelines Table 24.

PSPF Requirement 0080 mandates that 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.

- Dual citizenship does not preclude access to AUSTEO.
- If there is a business need to share AUSTEO information with a person who is not an Australian citizen, the originator can, on a case-by-case basis, reconsider application of the AUSTEO caveat to its information and, if warranted, apply a different caveat or classification to that information (e.g. the AGAO or REL caveat).

PSPF Requirement 0081 mandates that 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.

- AGAO material is releasable to appropriately cleared representatives of Five-Eyes foreign governments on exchange or long-term posting or attachment in the Australian Submarine Agency (ASA), ASD, ASIO, ASIS, the Department of Defence or ONI.

17.2.2 Information Access Controls

Robust technology systems provides access for personnel to undertake their work whilst also protecting information, technology and intellectual property.

Access to networks, operating systems, applications and security classified information that is processed, stored or communicated is controlled through:

- a clear understanding of the information held on such systems, and
- effective user identification and authentication practices.

See the PSPF Guidelines Section 13 for guidance on the technology system lifecycle.

17.2.2.1. User Identification, Authentication and Authorisation

PSPF Requirement 0134 mandates that 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.

The concepts of user identification, authentication and authorisation are closely related and interconnected, however, they are not interchangeable and are each distinct process that ensure the correct access is to resources is provided only to users that require it. These process are defined in Table 40 below:

Table 40: User Identification, Authentication and Authorisation

Process Type	Definition
Identification	The act of identifying a particular user, often through a username.
Authentication	The process of verifying the user's identity, often through a password or multi-factor authentication methods.
Authorisation	The process of granting a user access to services or systems, based on the identification and authentication already provided.

To ensure confidence in who is accessing their resources, entities should:

- establish a formal user registration and de-registration procedure for granting and revoking access
- regularly review user access rights to security classified information
- have uniquely identifiable users to ensure accountability
- authenticate the identity of users on each occasion that system access is granted, through multi-factor authentication methods as mandated by PSPF Requirement 0101, in accordance with ASD's Essential Eight mitigation strategies (see PSPF Guidelines Section 14.2.3), this includes for
    - higher-risk user such as system administrators, database administrators, privileged users and other similar positions of trust, and
    - remote access users
- implement authorisation measures allow entities to effectively control access to their resources and technology systems (including remote access), infrastructure and applications, and
- implement measures to manage authorised access to systems holding its security classified information as detailed in Table 41.

Table 41: Recommended Access Authorisation Measures

Type of Access	Recommended Measures
User access management	Ensure that systems for managing passwords are interactive and require users to follow good security practices in the selection and use of passwords or passphrases.
Authorised network access	• Consider the use of automatic equipment identification as a means to authenticate connections from specific locations and equipment. • Control physical and logical access to diagnostic and configuration ports. • Restrict the ability of users to connect to shared networks, including those that extend across entity boundaries. • Segregate groups of information services, users and information systems, based on an entity risk assessment. • Implement routing controls for networks to ensure computer connections and information flows do not breach other relevant access management measures.
Authorised operating system access	• Control access to operating systems through a secure log-on procedure. • Restrict and tightly control the use of utility programs that may be capable of overriding system and application controls. • Display restricted access and authorised use only (or equivalent) warnings upon access to all entity's technology systems, and shut down inactive sessions after a defined period of inactivity. • Consider restricting connection times to provide additional security for high risk applications.
Application and information access	Afford sensitive systems a dedicated (isolated) computing environment, in accordance with entity risk assessment.
Mobile computing and communications	Adopt security measures to protect against the risks of using mobile computing and communications facilities.

Recommended Approach

✔ Strengthen user identification, authentication and authorisation for higher-risk users by implementing additional personnel and physical security controls strategies.

17.3 Remote Access to Resources

A service-wide, principles-based approach to working flexibility in the Australian Public Service (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.

Recommended Approaches

- Establish procedures that take into consideration country-specific travel advice and guidance.
- Consult DFAT for practical advice, including on the availability of transfer and storage options using resources available through Australian Government embassies, high commissions and consulates.

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 remote allows personnel to work away from the office facilities and from alternate locations utilising remote technology systems. Examples of remote working include working from:

- a personal residence
- an entity facilities in another location (e.g. regional sites)
- another entity's facilities in Australia
- entity facilities where there is capability to provide sufficient protective security measures, for example offices operated by an entity's client or by a service provider contracted by the entity.

Entities should protect their resources commensurate with the assessed business impact level of their compromise, loss or damage. Entity physical assets are particularly vulnerable to loss outside of government facilities.

Entities should develop procedures to ensure appropriate accreditation of proposed work spaces outside of official entity facilities. This may require a security inspection of the proposed work space/site. The entity should considers the resources used or stored in the work space to determine whether:

- security classified information can be appropriately secured
- the work space can be independently secured
- the work space can be protected from oversight, or overhearing, by other people, including family and children (consider the other occupants in the residence), and
- all technology assets and resources being used can be secured or segregated from the entity's systems.

It may be difficult to secure entity information when the working environment is not controlled or managed by the entity. For example the work environment is:

- located inside commercial facilities or in private client facilities for which the entity is providing services
- the private residence of the entity's personnel
- the facility of an industry providing services to the entity to collect, use and/or store official information or other security protected Commonwealth resources.

Entities should treat any non-Australian Government facilities as Zone One areas for storage and/or use of Commonwealth information and resources unless the entity has:

- full control over the work space occupied by their personnel in commercial and client facilities
- confirmed appropriate physical and procedural security measures are in place for a higher level zone.

17.3.1.1. Working from Home

Working away from the office covers all work undertaken by personnel away from entity facilities, including using mobile device for home-based work.

PSPF Requirement 0136 mandates that entities consider the security risks of the environments in which their personnel operate, the type of information that will be used and how that information will be accessed as these can vary and may have a significant impact on security requirements.

PSPF Release 2024 (Section 17.3.1.1) mandates that 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). These requirements include working remotely with mobile devices.

Entities should establish procedures to ensure the entity's security measures to support home-based work are adequate to protect the entity's information and resources, including guidance on:

- what is and isn't allowed, including printing, cameras, microphones, use of social media, connecting to Wi-Fi networks and accessing websites
- what may and may not be shared with family members, house mates or other occupants of the residence and how to be aware of their surroundings to avoid accidental, incidental or deliberate viewing or overhearing information
- arrangements for transport and destruction of security classified information and resources, including mobile devices and removable media
- maximum storage periods in a residential location
- physical security measures, and
- reporting security concerns when working remotely.

See ASIO-T4 Security Managers Guide – *Private residence physical security assessment* (available on GovTEAMS).

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, information 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.

PSPF Requirement 0135 mandates that entities conduct a security risk assessment of the proposed location and work environment to inform decisions by the CSO to allow personnel to work in another government entity's facilities in Australia.

PSPF Requirement 0136 mandates that entities establish an agreement to manage the security risks associated with personnel working in another government entity's facilities in Australia.

Co-location or hosted arrangements must adhere to the minimum protections and handling requirements mandated in PSPF Requirement 0062. 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.

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 DFAT, and remote home-based work outside of an Australian Government entity facility, mission or post.

Recommended Approach

- Establish procedures that take into consideration country-specific travel advice and guidance.

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 (February 2007), 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 PSPF Guidelines Section 23.5—International Entity Facilities (including Missions and Posts).

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

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.

PSPF Requirement 0139 states that 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 CSO.

This means that 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 and resources. These minimum 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.

PSPF Requirement 0138 mandates that a security risk assessment of the proposed location and work environment informs decisions to allow personnel to work remotely in international locations. Each request to working remotely outside of an Australian Government facility, mission or post requires a risk assessment to determine whether the country and the proposed work environment (including the workspace, technology 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 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.

Recommended Approach

- Treat any non-Australian Government facilities as Zone One areas for the storage and/or use of security classified information and resources unless the entity has full control over the work space occupied by their personnel in commercial and client facilities and has confirmed appropriate physical and procedural security measures are in place for a high level zone.

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.

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.

Individuals must hold a security clearance commensurate with the security classification of the information, resources and activities they require access to.

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.

18.1.1 Security Clearance Levels

The Australian Government has four security clearance levels, noting that 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.

PSPF Release 2024 (Table 24) details the Australian Government security clearance levels required to access security classified information, resources and activities.

18.1.2 Security Clearance Status

There are four status levels for Australian Government security clearances—active security clearance, inactive security clearance, expired security clearance, and ceased security clearance.

See PSPF Release 2024 (Table 25) for details of the Australian Government Security Clearance status types and their definitions.

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.

PSPF Requirement 0140 mandates that the Australian Government Security Authorised Vetting Agency (AGSVA) conducts security vetting for Australian Government entities, unless the entity has been authorised to conduct security vetting for its own personnel, in a manner consistent with the Personnel Security Vetting Process and Australian Government Personnel Security Adjudicative Standard.

TOP SECRET-Privileged security vetting is conducted by the TOP SECRET-Privileged Access Vetting Authority.

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).

18.2.1 Competencies of Vetting Personnel

PSPF Requirement 0141 mandates that Authorised Vetting Agencies ensure vetting personnel (i.e. vetting analysts. and security clearance delegates) have and maintain the required skills and competencies for their role.

See PSPF Guidelines Section 1.5 for a list of current Authorised Vetting Agencies and detailed information on their responsibilities.

Vetting personnel should be able to demonstrate competencies and skills that include:

- knowledge of security clearance suitability assessments
- understanding of the security vetting process and the PSPF
- knowledge of the security environment and ability to use ASIO intelligence
- knowledge of and the ability to apply relevant public sector legislation, including espionage offences and the *Privacy Act 1988*
- knowledge of and the ability to apply the principles of natural justice and procedural fairness, and
- general skills and competencies, including:
    - handling official information
    - workplace communications
    - relevant interviewing skills
    - data analysis
    - administration, including records management.

The above 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 agency, qualifications be

obtained from a registered training organisation. A list of registered training organisations is available at www.training.gov.au.

18.3 Recognition of Existing Security Clearances

Where an individual holds, or has previously held, a security clearance issued by an Authorised Vetting Agency[15] 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 Entities must identify whether the clearance subject already holds, or has previously held, a security clearance, and advise the Authorised Vetting Agency accordingly.

PSPF Requirement 0142 mandates that the gaining Sponsoring Entity establishes new clearance conditions before assuming sponsorship of an existing security clearance that is subject to clearance conditions.

PSPF Requirement 0143 mandates that 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.

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) has exceed the limits outlined in PSPF Release 2024 (Table 26)
- 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
- the clearance was granted subject to clearance conditions, or
- the clearance has ceased.

18.4 Sponsoring Security Clearances

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

Organisations authorised by the Australian Government to sponsor security clearances include:

- members of the Defence Industry Security Program that may be authorised by the Department of Defence to sponsor security clearances up to Negative Vetting 2 level, and
- other organisations authorised by the Government Security Committee to sponsor security clearances.

Individuals are not eligible to sponsor a security clearance.

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. States and territories require an Australian Government entity to sponsor all Positive Vetting security clearances for their personnel.

[15] 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.

18.4.1 Identify and Record Positions that Require a Security Clearance

Personnel in certain positions may require a security clearance to access particular Australian Government resources (people, information and resources) relevant to their position. In accordance with an entity's physical and information security profile, this may include access to specific areas of an entity's facilities or specific technology systems.

An entity may also identify positions for which a security clearance is required, in addition to pre-employment screening and entity-specific checks, to provide a higher level of assurance about an individual's suitability. This may be appropriate for positions where:

- the occupant will have access to aggregations of information or resources, or
- the nature of the role requires greater assurance about the person's suitability, for example as a fraud mitigation or anti-corruption measure.

PSPF Requirement 0145 mandates that positions that require a security clearance and the level of clearance needed for that position are documented. This register of security clearances should identify:

- positions that require a security clearance for ongoing access to Australian Government information or resources
- positions that require a security clearance as a higher level assurance of personnel suitability, and
- when the requirement for a security clearance will be assessed (at least each time the position becomes vacant and before it is advertised).

PSPF Requirement 0155 mandates that entities must comply with the TOP SECRET-Privileged Access Standard if they identify positions requiring a TOP SECRET-Privileged Access clearance.

See PSPF Guidelines Section 20.1—Clearance Exemptions for Australian High Office Holders for guidance on the Australian public office holders who are exempt from holding a security clearance to access security classified information and resources.

See PSPF Guidelines Section 20.3—Members of Parliament (Staff) Act Employees for guidance on security clearance requirements for staff of ministers employed under Part III of the *Members of Parliament (Staff) Act 1984.*

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.

PSPF Requirement 0147 mandates that the individual's Australian citizenship is confirmed and pre-employment screening is completed before the entity seeks a security clearance for an individual in a position identified as requiring a security clearance.

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.

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.

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.

There are two types of eligibility waivers—citizenship and checkable background. Eligibility waivers are role-specific and not portable or transferrable and are subject to review.

The Accountable Authority (or CSO 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.

A person may not be granted a waiver for both the citizenship and checkable background requirements, as this would increase the security risks to an unacceptable level.

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.

PSPF Requirement 0148 mandates that 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. See PSPF Guidelines Section 18.6.3—Eligibility Waivers Risk Assessment.

PSPF Requirement 0149 mandates that the Accountable Authority (or the CSO if delegated) approves a citizenship eligibility waiver only after accepting the residual risk of waiving the citizenship requirement for that person, 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.

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. 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 must:

- disclose all relevant and required information,
- co-operate in the collection of personal documentation and corroborating evidence, and
- 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 employed to support and complement the capacities 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 not portable or transferrable.

DFAT 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 CSO 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.

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, and
- minimum personnel security checks.

In the security context, integrity is defined as a range of character traits that a clearance subject possesses (and demonstrates) in order for the government to have confidence in their ability to protect Australian Government information resources. These character traits are:

- **honesty** – truthful and frank and does not have a history of unlawful behaviour
- **trustworthiness** – responsibility, reliability and maturity
- **maturity** – capable of honest self-appraisal and able to cope with stress; age is not necessarily a good indicator of maturity
- **tolerance** – an appreciation of the broader perspective even when holding strong personal views, able to remain impartial and flexible (an ability to accept other peoples' life choices and respect cultures can indicate tolerance) and accept differences in people, opinions or situations through respect, understanding and empathy
- **resilience** – ability to adapt well in the face of adversity, trauma, tragedy, threats or significant sources of stress, and
- **loyalty** – a commitment to Australia and the democratic processes of the Australian Government. Loyalty is not confined to the nation but also includes the objectives, ethos and values of the working environment (strong political views incompatible with the Australian democratic system of government may put a person's loyalty in doubt).

Reference to a number of risk factor areas of the clearance subject's life, including personal relationships, employment history, behaviour and financial habits, contributes to an assessment of a clearance subject's integrity.

The assessment of a clearance subject needs to establish confidence that they possess a sound and stable character and that they are not unduly vulnerable to influence or coercion.

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.

Positive Vetting security clearances will be progressively replaced by TOP SECRET-Privileged Access security clearances, issued in accordance with the TOP SECRET-Privileged Access Standard.

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).

Authorised Vetting Agencies should only retain publicly accessible information that is directly related to, or reasonably necessary for, assessing the clearance subject's suitability to hold an Australian Government security clearance. Personal information (other than sensitive personal information) about a third party to the clearance subject should not be collected unless it is relevant to the clearance subject's suitability to hold a security clearance.

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

Recommended Approach

- Authorised Vetting Agencies comprehensively document information obtained through a digital footprint check because of the changing nature of online information.
- Information should have a relevant bearing on a clearance subject's suitability to hold a security clearance, including screenshots and direct links where possible.

19.2 Personnel Security Adjudicative Standard

PSPF Requirement 0154 mandates that entities assess the integrity (i.e. the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) of clearance subjects' eligibility and suitability to hold a Baseline, Negative Vetting 1, Negative Vetting 2 or Positive Vetting security clearance, in accordance with the Australian Government Personnel Security Adjudicative Standard.

Positive Vetting security clearances will be progressively replaced by TS-PA security clearances, issued in accordance with the TOP SECRET-Privileged Access (TS-PA) Standard.

The Australian Government Personnel Security Adjudicative Standard does not apply to TS-PA security clearances.

The Australian Government Personnel Security Adjudicative Standard details the common risk factor areas which establishes the context in which the determination of whether an individual is suitable to hold a security clearance, consistent with the national interest, is carefully considered. These risk factor areas are:

- external loyalties, influences and associations
- personal relationships and conduct
- financial considerations
- alcohol and drug use
- criminal history and conduct
- security attitudes and violations, and
- emotional and mental health issues.

Authorised Vetting Agencies are required to provide relevant information of concern obtained during the security vetting process to the Sponsoring Entity. See PSPF Guidelines Section 19.5.2.

Recommended Approach

- When determining suitability, Authorised Vetting Agencies should establish and use a process of structured professional judgement to come to an overall determination based on all the available information for a clearance subject.

19.2.1 TOP-SECRET Privileged Access

The TOP SECRET-Privileged Access Standard establishes the requirements that apply to TOP SECRET-Privileged Access clearances. The Standard is a classified document that is only available to qualified practitioners conducting TOP SECRET-Privileged Access vetting, psychological assessments or insider threat management activities in the TOP SECRET-Privileged Access Authority, Quality Assurance Office, or Sponsoring Entities (referred to as TOP SECRET-Privileged Access practitioners).

The TOP SECRET-Privileged Access Standard requires personnel who hold a TOP SECRET-Privileged Access security clearance to continue to demonstrate their trustworthiness and commitment to Australia, including by conducting themselves—in both their professional and personal lives—in a manner that is consistent with the attributes considered in the vetting process.

All personnel who obtain a TOP SECRET Privileged Access security clearance are provided with a copy of the annex to the TOP SECRET Privileged Access Standard that outlines their obligations for maintaining their security clearance, which include reporting requirements, approval of all overseas travel, and mandatory training requirements.

The TOP SECRET-Privileged Access Vetting Authority is required to assess an individual's suitability to hold TOP SECRET-Privileged Access security clearance by considering their trustworthiness and commitment to Australia, its values, and its democratic system of government in accordance with the TOP SECRET-Privileged Access Standard.

Additional information on these obligations is available from the insider threat team in each Sponsoring Entity.

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.

PSPF Release 2024 (Table 27) outlines the minimum personnel security checks required for each security clearance level.

Authorised Vetting Agencies should confirm that:

- all documents requiring signature and witnessing have been signed and that signatures and dates of signatures match
- details provided by the clearance subject match supporting documents
- referees are appropriate and their contact details are provided, and
- financial statements (if applicable) are provided and complete.

19.3.1 Identity Check

Authorised Vetting Agencies must verify the clearance subject'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.

Authorised Vetting Agencies should verify the identity of all clearance subjects in accordance with the National Identity Proofing Guidelines. Table 42 details the level of identity assurance required for each security clearance level.

Table 42: Levels of Identity Assurance for Security Clearances

Security Clearance Level	Level of Identity Assurance
Baseline	High assurance to **Level 3**
Negative Vetting 1	High assurance to **Level 3**
Negative Vetting 2	Very high assurance to **Level 4**
Positive Vetting	Very high assurance to **Level 4**

Levels of Assurance 3 and 4 constitute the following checks:

- 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
- the identity is not known to be used fraudulently, and
- only original physical documents shall be accepted (level 4).

See Identity Matching Services for information on how to access the Document Verification Service.

19.3.2 Confirmation of Australian Citizenship and Status of any Other Citizenships Check

Only Australian citizens are eligible to apply for an Australian Government security clearance, unless the citizenship eligibility requirement has been waived by the Accountable Authority of the Sponsoring Entity.

Evidence of other citizenships or nationalities may have bearing on one or more of the risk factors, including external loyalties, influences and associations.

Authorised Vetting Agencies must confirm the Australian citizenship details of a clearance subject and assess whether they hold any other citizenships.

19.3.3 Background Assessment Check

Authorised Vetting Agencies must assess a clearance subject's background for the relevant checking period. The relevant checking periods are detailed in Table 43 below.

Table 43: Relevant Checking Periods for Security Clearances

Security Clearance Level	Relevant Checking Period
Baseline	Five (5) years
Negative Vetting 1	Ten (10) years
Negative Vetting 2	Ten (10) years
Positive Vetting	Ten (10) years or from the age of 16, whichever is greater

Reasonable and available checking avenues in Australia or overseas include, but are not limited to, the following sources:

- corroboration from a credible referee
- government agencies and bodies
- academic institutions
- local Police records, if available (obtained domestically through liaison with the AFP or internationally through DFAT)
- humanitarian and aid agencies that maintain records for displaced persons
- places of worship, for birth, death and marriage information in lieu of government records
- private companies with whom the clearance subject has been employed, and
- the Department of Home Affairs for records of all Australian entries and exits.

An Authorised Vetting Agency should identify a clearance subject as having an uncheckable background when the vetting analyst cannot complete the required minimum checks and inquiries for the relevant period or the vetting analyst does not have sufficient confidence in the quantity, quality, credibility or reliability of the information provided. A background may be assessed as uncheckable because:

- the background assessment cannot be confidently conducted in certain countries of former residence
- certain documents do not exist (they never existed or no longer exist) or it is not possible to get copies from the issuing authority
- the source of the documents or information about the clearance subject may not be assessed as credible or reliable
- there are significant gaps in a clearance subject's background for which insufficient information is available, and/or the risks associated with these gaps are not readily able to be mitigated. A significant gap is considered to be greater than 12 months (cumulative) out of Australia within the background assessment period. Authorised Vetting Agencies are encouraged to assess the risk associated with uncorroborated gaps, taking into account the relevant checking period and the age of the clearance subject, as well as location(s) and length of period(s) out of Australia.

If the Authorised Vetting Agency has exhausted all reasonable and available checking avenues and determined that a clearance subject's background is uncheckable, they should:

- if there are no other concerns and identified risks can be mitigated - provide the Sponsoring Entity with information about the risks and mitigations relating to the clearance subject's uncheckable background in accordance with PSPF Requirement 0159 and request an eligibility waiver from the Sponsoring Entity (see PSPF Guidelines Section 18.6), and
- if there are other concerns or identified risks that cannot be mitigated, advise the Sponsoring Entity that the clearance cannot be progressed.

Separately, ASIO considers the background of clearance subjects as part of its security clearance suitability assessment. In some cases, ASIO will conclude an individual has an uncheckable background (e.g. because reliable security checking cannot be undertaken for the relevant countries) and will communicate this via a security clearance suitability assessment.

Recommended Approaches

- Authorised Vetting Agencies should use a questionnaire to gather initial background assessment information from clearance subjects.
- Authorised Vetting Agencies should document all attempts to satisfy the background checking requirement.
    - This includes alternative measures undertaken, any identified risks and how identified risks were mitigated (if mitigation is possible).
    - This information will inform any review process in the event of an adverse decision or inform the Sponsoring Entity's risk management in the event that a clearance is granted subject to waiver.

19.3.4 Acknowledgement of Relevant Legislation (Secrecy of Information) Check

Authorised Vetting Agencies must obtain acknowledgement from the clearance subject of their responsibilities for the protection of Australian Government information and resources.

An acknowledgement of relevant legislation (secrecy of information) confirms that those accessing Australian Government information and resources understand their roles and responsibilities to protect that information and resources. This includes the consequences of the misuse or disclosure of information and resources, and the application of criminal offences.

19.3.5 Referee Checks

Authorised Vetting Agencies must obtain referee reports about a clearance subject's eligibility and suitability to hold a security clearance. Table 46 below lists the referee check requirements for each security clearance level.

Table 44: Referee Check Requirements for Security Clearances

Security Clearance Level	Relevant Checking Period
Baseline	At least one professional referee
Negative Vetting 1	At least one professional referee and one personal referee
Negative Vetting 2	At least one professional referee, one personal referee and one un-nominated referee
Positive Vetting	At least one professional referee, one personal referee or peer referee, and one un-nominated referee

The referee reports should collectively cover the whole checkable period for all levels of security clearance.

- Professional referees—cover a period of at least the preceding three (3) months.
- Personal referees—cover the whole assessment period.

Additional referees may be required to collectively cover the whole checkable period. To competently comment on a clearance subject's character, referees are expected to have known the clearance subject for a minimum of three (3) months.

Professional and personal referees may be asked to provide information on a clearance subject's eligibility and suitability to hold a security clearance, as well as provide corroborating evidence in relation to other checks, including but not limited to:

- current and previous address
- current and previous employment
- overseas travel
- financial status, and
- use of alcohol and drugs.

Authorised Vetting Agencies should conduct at least one face-to-face referee interview, as sighting a photograph of the clearance subject may further establish identity, and assurance may be developed, that a referee has provided a full and truthful account of relevant information through non-verbal cues.

Authorised Vetting Agencies should not conduct telephone or email referee interviews if the referee is overseas in a high-risk location for hostile foreign intelligence activities. Entities may consult ASIO threat assessments for advice in this regard.

Close relatives, spouses, de-facto partners and purely professional contacts, such as doctors and teachers, may not be able to comment objectively on the clearance subject.

Current and past employers are well placed to confirm if a clearance subject has any security infringements, breaches or violations. A history of security incidents or breaches may indicate a disregard for security and highlight that the clearance subject's commitment to protecting Australian Government information and resources may be questionable.

Recommended Approach

- ✔ Authorised Vetting Agencies should contact previous government employers to determine if the clearance subject has previously been found to have breached the code of conduct, if there are current investigations into a possible breach of the code of conduct or if there are any integrity issues or identified concerns.

19.3.6 Digital Footprint Checks

Authorised Vetting Agencies must conduct a 'digital footprint' check. A digital footprint check includes conducting an open internet search on a clearance subject, as well as identifying and reviewing their publicly accessible social media.

A digital footprint is the unique pattern of electronic transactions made by an individual's online presence. An assessment of a clearance subject's digital footprint can provide insight into their life, interactions and personal views. However, recommendations on a security clearance outcome should not rely solely on information collected through a digital footprint check.

Information obtained from a digital footprint check can be combined with, or corroborate, other information obtained through personnel security vetting to provide assurance that a clearance subject has provided a full and truthful account of information relevant to the assessment of their integrity and, therefore, their suitability to

hold a security clearance. The value of information obtained can differ significantly between clearance subjects and is dependent on their online engagement.

The following guidance will assist Authorised Vetting Agencies to conduct digital footprint checks in a consistent manner and help to establish a picture of a clearance subject's digital footprint, including any online information or potential behaviours of concern that may require further checks or investigations.

19.3.6.1. Publicly Accessible Data

Online publicly accessible information refers to data that has been published online and is available publicly. This includes information obtained by virtue of general memberships, accounts on online social platforms or websites that are available to anyone.

Information is not publicly accessible if it is available only by connecting, 'friending', 'liking' or directly interacting with a clearance subject or third party to bypass privacy controls or access information limited by privacy settings.

The extent of information that is publicly accessible will depend on the scale of the clearance subject's social media presence and the privacy settings they have set on each platform.

Publicly accessible data collected about an individual may be defined as personal information for the purposes of the *Privacy Act 1988*.

Authorised Vetting Agencies must ensure that their policies and procedures for digital footprint checks comply with the information requirements in the *Privacy Act 1988*, the *Archives Act 1983* and any entity-specific legislation, including for the management and storage of online information collected through digital footprint checks.

19.3.6.2. Minimum Digital Footprint Checks

The digital footprint check is conducted against the factor areas of the Australian Government Personnel Security Adjudicative Standard. The factor areas of the standard assist in focusing digital footprint checks against relevant criteria.

Information obtained from a digital footprint check can be combined with, or corroborate, other information obtained through personnel security vetting to provide assurance that a clearance subject has provided a full and truthful account of information relevant to the assessment of their integrity and, therefore, their suitability to hold a security clearance.

A digital footprint check establishes an initial picture of a clearance subject's online presence. An initial picture of a clearance subject's digital footprint is obtained by applying the minimum required checks to a degree that is proportionate to the background check period of the clearance level, any identified risks and personnel security risk assessments that apply. The minimum required digital footprint checks and their associated rationales and search parameters are outlined in Table 45.

To conduct these checks effectively, Authorised Vetting Agencies need sufficient personal information about the clearance subject. This may include details of online aliases and accounts.[16] The level of information requested from a clearance subject and the extent of checks against this information should be proportionate to the level

[16] This could also include full names, AKAs, nicknames, handles, personas, email addresses, URLs as well as telephone numbers, addresses, car registration details and other identifiable details of online accounts managed by the clearance subject.

of clearance, the relevant background check period and any identified security concerns or risks about the clearance subject.

Table 45: Minimum Digital Footprint Checks

Check Type	Rationale	Search Parameters
Open search check	Enables a wide screening of online data, including: • content generated by or attributable to the clearance subject • financial, professional and personal interests • key associates or influences • legal or administrative proceedings • media relating to clearance subject, and • any other data relevant to the clearance subject's integrity.	Search terms • Subject's full name • Subject's email address(es) • Account names, aliases or handles provided by the clearance subject Time • Relevant background check period. Search engines • Any open search engine (e.g. Google, Bing, and Internet Archive).
Social media check	To provide information about the clearance subject's online behaviour and social networks, including: • posted content • 'shared' and 'liked' content (this should be viewed with caution, however, may it be useful if consistent with other information known about, or posts made by, the clearance subject) • participation in online communities and interest groups • pages or accounts followed, and • networking and interactions with other online persons or accounts.	Search terms • Subject's full name • Subject's email address(es) • Account names, aliases or handles provided by the clearance subject Time • Relevant background check period. Social media platforms • Facebook, Instagram, X, TikTok, LinkedIn, Snapchat, WeChat etc. • Any platforms the clearance subject has disclosed in the vetting process • Any platforms identified in the open search check.

The results of the minimum checks may indicate the need for more targeted searches to collect additional information. Targeted searches may also be warranted in response to identified security concerns or to corroborate information obtained through the vetting process.

Recommended Approach

- Authorised Vetting Agencies should corroborate and verify the integrity of the information if the digital footprint check identifies information of security concern.
- Issues in attributing information to the clearance subject should be raised with the clearance subject to provide them with an opportunity to clarify or provide further information.
- Authorised Vetting Agencies should account for missing or inaccurate information and the possibility of a clearance subject (or third party) sanitising or obfuscating their digital footprint to create a misleading impression.
- Discrepant information, or where it is apparent information obtained through a digital footprint check has been omitted by the clearance subject in other vetting checks (e.g. close associates of foreign nationality, significant life events and international travel or employment), should be resolved by the Authorised Vetting Agency.

19.3.6.3. Online Behaviour

A clearance subject's online activities, includes their posts, photos and associations form their online behaviours and may be indicators of security concerns. Vetting analysts may identify and flag for further investigation any online activity of potential interest that may call into question a clearance subject's integrity and, therefore, their suitability to hold a security clearance.

Vetting analysts should note that it can be difficult to establish the context of some online behaviour, for example, controversial web page searches may be for research purposes rather than for personal ideological reasons. Posts and comments in particular can be difficult to interpret without knowledge of a community's culture or influence.

Vetting analysts should flag for further investigation any online activity of potential interest to help provide additional context could mitigate the concerns identified against the relevant factor areas.

Examples of online behaviours that may be of security concern are described in Table 46.

Table 46: Examples of Online Behaviours that may be of Security Concern

Online Behaviours	Risk Factor Area(s)
Deliberate participation in or endorsement of ideological motivations that are anti-democratic, anti-rule of law or otherwise fundamentally undermine the rights of others to live in a free society.	External loyalties, influences and associations. Security attitudes and violations.
Indications of significant associations, activities or attitudes that draw into question the subject's loyalty to Australia.	External loyalties, influences and associations.
Appearing susceptible to, or easily succumbs to, groupthink or other conformity pressures, such as situations where the clearance subject continues to support dialogue that becomes intolerant, discriminatory or otherwise cruel.	Personal relationships and conduct. External loyalties, influences and associations.
Indications of poor reliability or trustworthiness such as flagrant dishonesty, consistent tardiness and absenteeism.	Personal relationships and conduct.
Media profile obtained through circumstances that may bring reputational harm.	Personal relationships and conduct.
Attitudes favouring inappropriate disclosure of sensitive or otherwise confidential information, the misuse of information technology systems and/or willfully contravening of rules or regulations governing the handling of security classified information.	Security attitudes and violations.
Images or information indicating impulsive or ostentatious purchases that suggests poor financial management, or indications the clearance subject is living above and beyond their financial means.	Financial considerations.
Indications of inappropriate use of alcohol or drugs.	Alcohol and drug usage.
Engaging in criminal activity or deliberate rule violations.	Criminal history and conduct. Security attitudes and violations.

19.3.7 National Police Check/Criminal History Check

Authorised Vetting Agencies must obtain a national Police check for the clearance subject.

A national Police check is carried out by AFP in accordance with the Spent Conviction Scheme. The scheme allows the clearance subject to withhold disclosure of spent convictions unless exclusion has been granted.

The application of the Spent Conviction Scheme for relevant clearance levels is as follows:

Table 47: Referee Check Requirements for Security Clearances

Security Clearance Level	Application of the Spent Conviction Scheme
Baseline	A 'No Exclusion' national Police check/Police records check. Under a 'No Exclusion' check, clearance subjects are not required to divulge convictions subject to the following conditions: • it has been ten (10) years from the date of the conviction o or five years for juvenile offenders • the individual was not sentenced to imprisonment for more than 30 months • the individual has not re-offended during the ten (10) year waiting period, and o or 5 years for juvenile offenders • a statutory or regulatory exclusion does not apply.
Negative Vetting 1	A 'Full Exclusion' national Police check/Police records check. Under a 'Full Exclusion' check, clearance subjects are required to detail all convictions, regardless of the date of conviction or nature of offence, as well as any cases currently pending or before the courts.
Negative Vetting 2	Same as for Negative Vetting 1
Positive Vetting	Same as for Negative Vetting 1

See OAIC's Criminal Records Commonwealth Spent Convictions Scheme for further information.

19.3.8 Financial History Assessment Check

Authorised Vetting Agencies must conduct a financial history assessment check. The purpose of this assessment is to consider whether:

- the clearance subject is living beyond their means, for example spending more than they earn or is impulsive and irresponsible with their spending
- there is any history of unmanaged debt, or
- the clearance subject has failed to meet financial obligations, including submission of tax returns, payment of rent and debts, bankruptcy and denial of credit.

Additional checks may be warranted on a case-by-case basis where there are concerns about a clearance subject's financial situation, particularly unexplained wealth or a high level of debt.

The Authorised Vetting Agency may seek a credit history check from an accredited financial credit check organisation if a clearance subject has a history of financial defaults, is in a difficult financial situation or if there are concerns about the clearance subject's finances,

Recommended Approach

- The Authorised Vetting Agency should request a bankruptcy check in writing through the Insolvency and Trustee Service Australia, where a clearance subject has indicated that they have been bankrupt or insolvent.

19.3.9 Financial Statement Check

Authorised Vetting Agency must request that clearance subjects complete a financial statement for Negative Vetting 1 and above clearance levels.

A financial statement provides a detailed summary of a clearance subject's assets, income, liabilities and expenditure. It can help identify if a clearance subject is financially overextended.

Recommended Approach

- Vetting analysts should undertake specialist training or seek specialist advice before undertaking complex financial analysis.

19.3.10 Financial Probity Assessment Check

Authorised Vetting Agency must undertake a probity assessment into a clearance subject's financial circumstances for Positive Vetting clearance levels.

A financial probity assessment builds on a financial history check and financial statement (with supporting documents) by undertaking a more rigorous evaluation of a clearance subject's financial circumstances to establish, beyond reasonable doubt, whether there are any characteristics of financial vulnerability. For example, crime or indicators of financial difficulty, unexplained wealth or gambling habits.

19.3.11 Comprehensive Financial Assessment Check

Comprehensive financial assessment checks are only a mandatory requirement for TOP SECRET-Privileged Access security clearances and must be conducted in accordance with the TOP SECRET-Privileged Access Standard.

19.3.12 ASIO Security Clearance Suitability Assessment Check

Authorised Vetting Agency must obtain an ASIO Security Clearance Suitability Assessment (SCSA) for Negative Vetting 1 and above clearance levels, or lower levels where concerns have been identified that may impact on the national interest.

Authorised Vetting Agency must request the ASIO security clearance suitability assessment after all other checks and the security clearance interview (if required) are complete. This prevents unnecessary use of ASIO resources where the clearance subject would not otherwise be recommended for a clearance.

At any time, ASIO may provide preliminary advice to an Authorised Vetting Agency regarding the subject of an ASIO security clearance suitability assessment pending the issue of that assessment.

ASIO can initiate a new security clearance suitability assessment at any time in response to new information.

Part IVA of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) provides for ASIO to undertake security clearance suitability assessments of people. For the purposes of security clearances, the ASIO security clearance suitability assessment provides a recommendation to the Authorised Vetting Agency on a person's suitability to hold a security clearance, and may provide additional advice including advice on conditions that might be placed on a clearance. ASIO takes into account matters such as the subject's activities, associates, attitudes, background and character. The ASIO assessment is based on:

- information provided by the subject, employing entity and Authorised Vetting Agency
- ASIO's intelligence holdings, including its assessment of security threats, and where necessary,
- may involve an ASIO interview of the subject and other inquiries.

Sub-section 82E(3) of the ASIO Act permits Authorised Vetting Agencies to take appropriate action (such as temporarily suspending a person's security clearance and preventing ongoing access to classified information) if the Authorised Vetting Agency is satisfied, on the preliminary advice from ASIO, that it is necessary to take that action as a matter of urgency due to requirements of security.

Section 82E of the ASIO Act requires that any such action is temporary, pending receipt of an ASIO security clearance suitability assessment. Other than pursuant to the exception contained in subsection 82E(3), the

ASIO Act prevents Authorised Vetting Agencies from making, or refraining from making, a security clearance decision in respect of a person on the basis of any communication from ASIO that does not amount to a full security clearance suitability assessment.

ASIO will liaise with the relevant Authorised Vetting Agency when intending to provide preliminary advice under section 82E of the ASIO Act, including where an ASIO review of an existing security clearance suitability assessment indicates security concerns.

ASIO may also communicate with a State security Authorised Vetting Agency if the Director-General of Security is satisfied that the requirements of security make it necessary as a matter of urgency for the State security Authorised Vetting Agency to make a security clearance decision in respect of the person.

While it is within ASIO's functions to furnish security clearance suitability assessments directly on States or authorities of States under subsection 82F(2) of the ASIO Act, subsection 82F(3) stipulates that ASIO is prohibited from furnishing to a State or an authority of a State, other than in the form of a security clearance suitability assessment, any information concerning a person which ASIO knows is intended or likely to be used by the State or an authority of the State in considering whether to make, refuse to make, or refrain from making a security clearance decision in respect of the person.

Recommended Approach

- ✔ Authorised Vetting Agencies should negotiate with ASIO on a case-by-case basis where operational needs require the ASIO security clearance suitability assessment to be conducted concurrently with other checks.

19.3.13 Security Interview Check

Authorised Vetting Agencies must conduct security interviews of clearance subjects addressing the requirements listed below.

Table 48: Security Interview Check Requirements for Security Clearances

Security Clearance Level	Security Interview Requirements
Baseline	Interview not required, unless: • the citizenship or background check requirements have been waived , or • there are particular suitability concerns about a clearance subject.
Negative Vetting 1	Same as for Baseline.
Negative Vetting 2	Face-to-face or virtual via secure platform (or telephone in exceptional circumstances) interview required, addressing: • external loyalties, influences and associations • personal relationships and conduct • financial considerations • alcohol and drug use • criminal history and conduct • security attitudes and violations, and • emotional and mental health issues.
Positive Vetting	Same as for Negative Vetting 2

Authorised Vetting Agencies should conduct supplementary interviews that address the specific areas of concern for all clearance levels where specific areas of concern arising from internal and external checking have not been adequately resolved by other supplementary checks.

If any further concerns are identified, Authorised Vetting Agencies should conduct supplementary interviews:

- face-to-face for significant or complex issues, and
- via video or telephone for resolve minor issues (e.g. the clearance subject is travelling overseas) or where a face-to-face interview is not possible.

Telephone interviews are not to be conducted if the individual seeking a clearance is overseas in a high-risk location for hostile foreign intelligence activities. Entities can consult ASIO threat assessments for advice in this regard.

Recommended Approach

- ✔ Face-to-face, video or telephone interviews should address all factor areas in the Australian Government Personnel Security Adjudicative Standard and any specific areas of concern.

19.3.14 Psychological Assessment Check

Authorised Vetting Agencies must obtain a psychological assessment for Positive Vetting clearance subjects. A typical psychological assessment consists of two parts:

- psychometric testing, and
- a psychological interview.

Psychological assessments identify any psychological risks associated with the subject as an input to determine general suitability and may point to any potential security risks.

Psychological assessments are undertaken by appropriately qualified psychologists and are mostly used to establish a clearance subject's suitability for a Positive Vetting clearance. See the Psychology Board of Australia's website to search for qualified Psychologist or check their registration status or qualifications.

19.3.15 Overseas Travel Check

Overseas travel checks are only a mandatory requirement for TOP SECRET-Privileged Access security clearances and must be conducted in accordance with the TOP SECRET-Privileged Access Standard.

Most Authorised Vetting Agencies elect to do overseas travel checks for Negative Vetting 1 and above security clearances. This check will be mandated in PSPF Release 2025 as part of the personnel security vetting upgrades.

19.3.16 Statutory Declaration (only when vetting is conducted by a state or territory agency)

When vetting is conducted by a Commonwealth state or territory agency, clearance subjects must sign a statutory declaration to provide legal verification that the information provided is truthful and complete and documents are accurate and without amendments, issued by the issuing authority and relate to the clearance subject.

The clearance subject may make a statutory declaration in lieu of some supporting documents where:

- copies of documents cannot reasonably or readily be obtained from the issuing authority within the required time, or
- a reasonable delay is expected and the clearance subject undertakes to provide the documents as soon as they are received.

Commonwealth state or territory agency Authorised Vetting Agencies should not accept a statutory declaration for:

- primary identification documents issued by an Australian authority
- proof of current employment

- proof of current residential address
- primary identification documents issued by a foreign authority where it is possible to obtain these documents, or
- corroboration of gaps identified in determining a clearance subject's checkable background.

See AGD's Statutory Declarations for further information.

19.3.17 Additional Personnel Security Checks

Authorised Vetting Agencies may elect to conduct additional vetting checks or assessments where they have access to additional capabilities or where the check or assessment is relevant to addressing any concerns identified or not able to be resolved through the minimum personnel security checks.

Table 49 provides two examples of additional vetting checks that may be undertaken for security clearances.

Table 49: Examples of Additional Personnel Security Checks

Additional Check	Rationale
Criminal intelligence check	A criminal intelligence check involves the use of non-conviction-related information to identify whether an individual has links to criminality, including involvement in or association with those involved in serious and organised crime. A criminal intelligence check includes consideration of pre-prosecution information, criminal intelligence and criminal affiliations. Information indicating an individual is involved in, or associates with, those involved in serious and organised crime may indicate a lack of judgement or discretion, or susceptibility to undue influence, coercion, exploitation or duress. Such information raises questions about the individual's suitability to hold a security clearance.
Mental health check	A mental health condition does not necessarily indicate that a clearance subject would not be able to protect Australian Government resources. Where there is a concern that the clearance subject's emotional stability or psychological health may affect their ability to protect Australian Government resources, the Authorised Vetting Agency obtain advice from a duly qualified mental health practitioner. If the clearance subject is, or has been, under treatment for an emotional or mental health condition, information may be requested from the treating mental health professional with the specific consent of the clearance subject. It may be necessary for the Authorised Vetting Agency to seek independent medical advice from a mental health professional if the clearance subject does not have their own practitioner or if the concern is unrelated to current or previous treatment.

19.4 National Interest

The national interest is Australia's sovereignty, security, prosperity, economic, military and culture ambitions, and social cohesion of the nation and its people.

PSPF Requirement 0157 mandates that a clearance subject's eligibility and suitability to hold a security clearance assessment resolving any doubt in the national interest.

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 about whether they are loyal to the Australian Government.

Conflict of views or conscientious objections could arise in some cases. When a clearance subject acts in ways that indicate 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 risk factor areas outlined in the Australian Government Personnel Security Adjudicative Standard.

See PSPF Guidelines Section 19.2—Personnel Security Adjudicative Standard.

19.5 Security Vetting Outcomes

The outcome of a security vetting process is a determination of the clearance subject's eligibility and suitability to hold a security clearance based on an assessment:

- against the Australian Government Personnel Security Adjudicative Standard (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.

The Authorised Vetting Agency should provide a summary of information when notifying the clearance subject and Sponsoring Entity of the security clearance outcome. This includes:

- the level of clearance the subject is being assessed against
- the date of the determination of ineligible, granted, granted–conditional, denied or cancelled
- any eligibility (background or citizenship) waiver granted in the clearance process and any conditions placed by virtue of the waiver
- any conditions required as part of a granted–conditional clearance
- the date for revalidation, and
- details of the review and appeals processes open to the clearance subject, if applicable.

See PSPF Release 2024 (Tables 28 and 29) for descriptions of security vetting determinative and administrative outcomes.

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. Clearance conditions may include access restrictions or other risk mitigations measures.

PSPF Requirement 0158 mandates that 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, and

- 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 CSO, however the CSO is required to notify the Accountable Authority of the clearance conditions.

Conditions may be placed on a clearance at the instigation of the Sponsoring Entity, or the Authorised Vetting Agency, or on the recommendation of ASIO's security clearance suitability assessment.

19.5.2 Security Vetting Outcomes Summary of Information

Authorised Vetting Agency should provide a summary of information when notifying the clearance subject and Sponsoring Entity of the security clearance outcome. This includes:

- the level of clearance the subject is being assessed against
- the date of the determination of ineligible, granted, granted–conditional, denied or cancelled
- any eligibility (background or citizenship) waiver granted in the clearance process and any conditions placed by virtue of the waiver
- any conditions required as part of a granted–conditional clearance
- the date for revalidation, and
- details of the review and appeals processes open to the clearance subject, if applicable.

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 that raise concern over the protection of security classified information, resources or activities from compromise, espionage, sabotage, foreign interference etc.) and information of non-security concern (such as integrity or allegiance to Australia or the Australian Government's interest).

Sponsoring Entities are the critical repositories of information about a clearance holder's current circumstances and are best placed to provide the most current security-related information to the Authorised Vetting Agency.

Effective information sharing over the life of a security clearance will also make it easier for clearance holders and Authorised Vetting Agencies to compile the necessary information to conduct a revalidation of a security clearance.

Where changes in circumstances and other information relevant to determining a person's eligibility or suitability to hold a security clearance, have already been considered by the Authorised Vetting Agency at the time they occurred, these assessments can inform the vetting analyst's determination at revalidation. Authorised Vetting Agencies must share information of security concern about security clearance holders with Sponsoring Entities. This allows Sponsoring Entities to manage risks related to the clearance holder's ongoing access to Australian Government resources.

PSPF Release 2024 mandates several requirements on the sharing of information of security concern during a clearance subject's vetting process, outlined below:

- PSPF Requirement 0167 mandates that the Sponsoring Entity shares relevant information of security concern, where appropriate.
- PSPF Requirement 0177 mandates that the Sponsoring Entity shares relevant information of security concern, where appropriate with the Authorised Vetting Agency.

- PSPF Requirement 0178 mandates that the Authorised Vetting Agency shares information of security concern about security clearance holders with the Sponsoring Entity.
- PSPF Requirement 0179 mandates that the Authorised Vetting Agency assesses and responds to information of security concern about security clearance holders, including reports from Sponsoring Entities.
- PSPF Requirement 0177 mandates that entities share all information of security concern. The assessment of whether information is of security concern can only be made by the entity assessing that concern. Therefore, all information pertaining to personnel is shared between Sponsoring Entities and Authorised Vetting Agencies so that they can determine whether it is relevant.

Recommended Approach

- ✔ Authorised Vetting Agency should establish effective procedures to document and share adverse information with Sponsoring Entities. This includes procedures to identify mitigation activities that Sponsoring Entities could undertake to manage risks in relation to the clearance subject's ongoing suitability.

19.6.1 Concerns about Existing Clearance Holders

A vetting analyst or delegate may deny or revoke a security clearance during the security vetting process if a personnel's available information reflects a current or recurring pattern of reliable or significant adverse information.

If, after evaluating the information of security concern, the vetting analyst or delegate decides that the security concern is not serious enough to warrant a determination to revoke or downgrade the security clearance, the Authorised Vetting Agency should notify the clearance subject and their Sponsoring Entity that future incidents of a similar nature may result in revocation of the security clearance. This information is recorded in the clearance subject's personal security file.

When information of security concern becomes known about a clearance subject who currently has access to Australian Government resources, and before determining whether to revoke or downgrade an existing clearance, the vetting analyst and the delegate considers whether the person:

- voluntarily reported the information
- responded to questions truthfully and completely
- sought assistance and followed professional guidance, where appropriate
- resolved or appears likely to favourably resolve the security concern, and
- has demonstrated positive changes in behaviour and employment.

19.7 Procedural Fairness

PSPF Requirement 0160 mandates that Authorised Vetting Agencies apply 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. When the principles of procedural fairness are applied in a security clearance process, it reduces the possibility of the process being compromised and a new clearance process being ordered on review or appeal.

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 these guidelines.

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 an opportunity to respond before the final recommendation is made. It is recommended that any information used to make a decision be substantiated, particularly when the information is from a referee who may be biased or have a conflict of interest.

Authorised Vetting Agencies should provide the clearance subject with a written statement identifying any concerns. It is recommended that Authorised Vetting Agencies give the clearance subject a reasonable period (normally two weeks from the date of advice) to respond to the concerns before a final recommendation is made. It is recommended that the clearance subject's response be provided to the delegate so they may make an informed decision based on all the material available.

Separate arrangements ensure procedural fairness and national security are preserved where denial of a clearance is based on an ASIO security clearance suitability assessment.

Recommended Approach

- ✔ Authorised Vetting Agency should consider whether an outsourced vetting service provider is able to manage procedural fairness issues involving outsourced vetting services.

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, it is recommended that Authorised Vetting Agencies tell the clearance subject the case to be met (to the fullest extent possible consistent with national security) and give them an opportunity to reply before the delegate makes a decision.

It is also recommended that Authorised Vetting Agencies ensure that the clearance subject:

- is told the case to be met 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 negative information an Authorised Vetting Agency has about the clearance subject be disclosed to the extent possible consistent with national security. It is sufficient that a summary of the information being considered be 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
- does not bring, or appear to bring, a biased or prejudiced mind to making the decision.

A delegate must be impartial. PSPF Release 2024 (Section 19.7.1) mandates that Authorised Vetting Agencies maintain processes to ensure application of the bias rule to comply with administrative law principles.

19.7.2 Procedural Fairness and Delegate

PSPF Release 2024 (Section 19.7.2) mandates that 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

PSPF Release 2024 (Section 19.7.3) mandates that 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:

- being told the case to be met (e.g. that an agency is considering denying, 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

PSPF Release 2024 (Section 19.7.4) mandates that 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. See PSPF Release 2024 (Table 30) for the administrative review process.

Security clearance decisions made by ASIO may be internally reviewable and reviewable by the Administrative Appeals 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 Appeals 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 Appeals Tribunal. For information about how to apply for a review of a decision in the Security Division, see the Administrative Appeals Tribunal website.

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 1998* in the way information was handled
- 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 Commonwealth of Australia Constitution Act.

20 High Office Holders and their Support Staff

20.1 Clearance Exemptions for Australian High Office Holders

Some Australian high office holders are not required to hold a security clearance to access security classified information while exercising the duties of the office. Staff of these office holders are not exempt from security clearance requirements.

Australian office holders who do not need a security clearance are:

- members and senators of the Commonwealth (including Ministers, shadow ministers and backbenchers[17]) 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 Appeals Tribunal.

20.2 PSPF Obligations for Australian High Office Holders

An Australian high 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).

Once such determination, the Special Minister of State Determination 2023/12, requires that electorate or personal staff (ministerial staff) employed under Part III of the MOP(S) Act by Ministers obtain and maintain a Negative Vetting 2 security clearance.

The Australian Government Security Authorised Vetting Agency is the Authorised Vetting Agency responsible for the security clearances of ministerial staff.

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 in the PSPF Release 2024 (Table 31).

[17] Backbencher is a Member of Parliament who is not a minister or special officer holder.

20.3.1 Roles and Responsibilities

In addition to PSPF Release 2024 (Table 31), each stakeholder (Department of Finance, the Department of State or delegate, or the Minister/Chief of staff) has supporting responsibilities they must meet, outlined in the following subsections.

20.3.1.1. Commencement of Ministerial Staff

The Minister or Chief of Staff advises the Department of Finance of the commencement of a new ministerial staff member and, where the Minister has responsibilities across multiple portfolios, advises which portfolio is most relevant to the work of the staff member.

Entities are not required to undertake pre-employment screening for ministerial staff.

20.3.1.2. Temporary Access for Ministerial Staff

If the new ministerial staff member requires temporary access to security classified information and resources prior to gaining a security clearance:

- Minister or Chief of Staff submits a written request to the Department of State for temporary access to security classified information and resources and includes advice about the relative benefit of the individual being granted temporary access prior to finalising the clearance process
- Department of State conducts a risk assessment before granting temporary access and weighs the findings against the Minister's advice on the relative benefits of approving the requests
- Department of State advises the Minister of its findings, including any identified risks, and
- Minister or Chief of Staff considers the Department of State's findings and provides the Department of State with written confirmation to acknowledge and accept any identified risks and commit to supervising access
- where approved, the Department of State grants temporary access to security classified information and resources.

20.3.1.3. Security Clearance Process for Ministerial Staff

The Special Minister of State Determination 2023/12 requires that staff of Ministers employed under Part III of the MOP(S) Act obtain and maintain a Negative Vetting 2 security clearance. See PSPF Guidelines Section 20.3.2—Variation of Special Minister of State's Determination for a Minister's electorate officer for guidance on varying these security clearance requirements.

The Department of Finance initiates the security clearance process and advises the relevant Department of State, then:

- Department of State declares an interest in the individual's security clearance with AGSVA, and
- Minister or Chief of Staff encourages the new ministerial staff to submit their security clearance paperwork, supporting documentation and subsequent advice on changes of personal circumstances in a timely manner.

20.3.1.3.1. Eligibility Waivers for Ministerial Staff

Where an eligibility waiver either for citizenship or a checkable background is required for the security clearance process to continue:

- AGSVA advises the Department of Finance

- Department of Finance advises the relevant Department of State
- Department of State considers the risks and seeks advice from the Minister or Chief of Staff on whether to support an eligibility waiver or terminate the security clearance process
- Department of State advises the Department of Finance whether the eligibility is supported
- Department of Finance provides AGSVA with the paperwork to support the eligibility waiver or discontinue the security clearance process, and
- Department of State reviews the eligibility waiver annually.

20.3.1.3.2. Security Clearance Conditions for Ministerial Staff

Where a security clearance may only be issued with additional conditions:

- AGSVA advises the Department of Finance
- Department of Finance advises the Department of State
- Department of State considers the risks and seeks the agreement of both the Minister or Chief of Staff and the clearance subject
- Department of State advises the Department of Finance whether the conditions have been agreed by all parties
    - If the Department of State, the Minister or the clearance subject do not agree with the conditions advised by AGSVA, the ministerial staff member will be unable to obtain a security clearance
- Department of Finance will advise AGSVA whether all parties have agreed to the conditions or to discontinue the clearance process, and
- Department of State reviews the conditions annually.

20.3.1.3.3. Ongoing Suitability of Ministerial Staff

The Department of State monitors and manages the ongoing suitability of the ministerial staff of their portfolio ministers. This includes providing:

- annual security awareness training
- security briefings and advice
- annual security appraisals, and
- a review of waivers and any conditions attached to the clearance.

The ministerial staff member advises the Department of State of any relevant changes in their personal circumstances. The Department of State provides this information to AGSVA.

The Department of State (at the discretion of the Accountable Authority) shares any security risks identified during the ongoing assessment of the ministerial staff member with the Minister or Chief of Staff.

20.3.1.3.4. Separation of Ministerial Staff

The Minister or Chief of Staff advises the Department of Finance of the separation of ministerial staff through timely submission of termination forms, including advising where cessation of employment is the result of misconduct other adverse circumstances.

The Department of Finance then:

- notifies both the Department of State and AGSVA of the separation of ministerial staff and whether the cessation is the result of misconduct or other adverse reasons, and
- manages the transfer of ministerial staff between ministerial offices and advises both the losing and gaining Departments of State.

The Department of State debriefs the separating ministerial staff member, advises them of their continuing security obligations and removes access to entity information and resources.

20.3.2 Variation of Special Minister of State's Determination for a Minister's electorate officer

The Special Minister of State Determination 2023/12 requires that staff of Ministers employed under Part III of the MOP(S) Act obtain and maintain a Negative Vetting 2 security clearance. Under the Determination, in exceptional circumstances, a Minister's Chief of Staff may request a variation of the security clearance requirement from the Secretary of the Department of Home Affairs.

See the Request to Vary Ministerial Staff Security Clearance Requirements Form below.

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.

Request to Vary Ministerial Staff Security Clearance Requirements Form

The Special Minister of State Determination 2023/12 allows a Minister's Chief of Staff to request a variation of the security clearance requirement from the Secretary of the Department of Home Affairs. The Secretary, Department of Home Affairs will consider a request to vary the requirement for a Negative Vetting Level 2 security clearance following endorsement by the Department of State.

Section 1: Request - Completed by Requesting Minister's Chief of Staff

I certify that	Name of Electorate Officer	an electorate officer for	Minister's name
is not required to access, and will not come into contact with, TOP SECRET security classified material. I request a variation of the requirement for the above electorate officer to hold a Negative Vetting 2 security clearance.			
Name of Chief of Staff	Phone Number	Signature	Date

Forward request to the Chief Security Officer or delegate of the Department of State.

Section 2: Endorsement - Completed by the Sponsoring Department of State

Name of Department of State			
I endorse the request to vary the requirement for a Negative Vetting 2 security clearance for the above mentioned electorate officer. I confirm they will not have access to TOP SECRET material, and may have access to or come in contact with security classified material (tick whichever is applicable): ☐ at or below PROTECTED ☐ at SECRET			
Name of Endorsing Officer	Phone Number	Signature	Date
Position of Endorsing Officer			

Submit endorsed request to the Department of Home Affairs at PSPF@homeaffairs.gov.au

Section 3: Approval - Completed by the Secretary of the Department of Home Affairs (or their delegate)

As the delegate for the Secretary, Department of Home Affairs, I vary the requirement for the above mentioned electorate officer to be security cleared to Negative Vetting, subject to them undergoing (tick whichever is applicable): ☐ Baseline ☐ Negative Vetting 1 ☐ Variation not approved - Negative Vetting 2 required		
Name of Approving Officer	Position of Approving Officer	Date

Send approved request to Ministerial and Parliamentary Services, Department of Finance at mpshelp@finance.gov.au

21 Maintenance and Ongoing Assessment

Effectively assessing and managing ongoing suitability ensures that entity personnel, including contractors, continue to meet requirements established at the point of engagement.

Entitles must maintain confidence in their personnel's ongoing suitability to access Australian Government information and resources, and manage the risk of malicious or unwitting insiders.

The TOP SECRET-Privileged Access Standard includes additional specific requirements for assessing and managing the ongoing suitability of TOP SECRET-Privileged Access security clearance holders. The Standard is a classified document that is only available to qualified practitioners conducting TOP SECRET-Privileged Access vetting, psychological assessments or insider threat management activities in Authorised Vetting Agencies or Sponsoring Entities (referred to as TOP SECRET-Privileged Access practitioners).

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.

Accountable Authorities are responsible for determining their entity's risk tolerance and managing the security risks of their entity, including as they relate to the ongoing suitability of personnel to access Australian Government information and resources.

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 PSPF Guidelines Section 20.3.

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.

See PSPF Guidelines Section 1.5 for a list of current Authorised Vetting Agencies and detailed information on their responsibilities.

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.

See PSPF Guidelines Section 19.6 for further guidance.

21.2.2 Assess and Respond to Information of Concern

PSPF Release 2024 (Section 21.2.2) mandates that Authorised Vetting Agencies must assess and respond to information of concern about security clearance holders, which includes reports from Sponsoring Entities.

See PSPF Guidelines Section 19.6 for further guidance.

21.2.3 Review Conditional Security Clearances

PSPF Requirement 0161 mandates that the Authorised Vetting Agency must review the conditions for conditionally 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.

See PSPF Guidelines Section 19.5.1 for further guidance.

21.2.4 Review for Cause

PSPF Requirement 0162 mandates that 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.

21.2.4.1. ASIO-Initiated Review of ASIO Security Clearance Suitability Assessment

Sub-section 82E(3) of the ASIO Act permits Commonwealth Authorised Vetting Agencies to take appropriate action (such as temporarily suspending a person's security clearance and preventing ongoing access to classified information and resources) if the Authorised Vetting Agency is satisfied, on the preliminary advice from ASIO, that it is necessary to take that action as a matter of urgency due to requirements of security.

See PSPF Guidelines Section 19.3.12 for further information on ASIO security clearance suitability assessments.

21.2.5 Implement TSPA Standard

In accordance with PSPF Requirement 0163, Authorised Vetting Agencies are to implement specific requirements in the TOP SECRET-Privileged Access Standard to assess and manage the ongoing suitability of TOP SECRET-Privileged Access 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 TOP SECRET-Privileged Access security clearances, reviews for cause, and revalidation of TOP SECRET-Privileged Access security clearances in accordance with the timeframes specified in the TOP SECRET-Privileged Access Standard.

See PSPF Guidelines Section 19.2.1 for further guidance.

21.3 Sponsoring Entities Maintenance Responsibilities

Entities must share relevant information of security concern. The assessment of whether information is relevant or of security concern can only be made by the entity assessing that concern. Sponsoring Entities and 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.

21.3.1 Procedures for Assessing Managing Ongoing Suitability

PSPF Release 2024 (Table 33) identifies entity procedures to assess and manage the ongoing suitability of personnel. Some of these may be built into existing performance management procedures.

Recommended Approach

- An entities' procedures for assessing and managing the ongoing suitability of personnel include periodic employment suitability checks, as well as mechanisms to support reporting of concerns.

21.3.1.1. Security Clearance Maintenance

Security clearance maintenance requirements are in addition to ongoing suitability measures that apply for all personnel.

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. See PSPF Guidelines Sections 1.5 and 1.6 for details on the respective roles and responsibilities of Authorised Vetting Agencies and Sponsoring Entities for security clearance maintenance; this includes clearance conditions for holders of conditional security clearances and clearances subject to eligibility waivers.

For security cleared personnel:

- 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.
- Authorised Vetting Agencies are responsible for assessing how information relates to an individual's eligibility and suitability to hold a clearance.

PSPF Requirement 0167 mandates that Sponsoring Entities 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.

21.3.1.2. Performance Management

Entity performance management programs provide an avenue for supervisors and line managers to assess and report on the ongoing performance of personnel. Performance management programs may also be used for the assessment and management of ongoing suitability, including identifying personnel who display behavioural concerns such as disregard for entity security procedures.

Entities are encouraged to embed security considerations into their annual performance appraisals by seeking confirmation that:

- individuals have reported any change of circumstances, such as changes to details provided during the pre-employment screening (e.g. criminal charges)

- individuals have reported any 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)
- real or perceived conflicts of interest
- line managers that there are no unreported security concerns about the individual.

Where security concerns are identified as part of performance management, entities are encouraged to undertake additional employment suitability checks to assess whether the concerns are relevant to the person's ongoing suitability to access Australian Government resources. Identifying security concerns may trigger incident reporting obligations under the PSPF.

For security clearance holders, security concerns could affect their eligibility and suitability to hold a security clearance.

Central human resources areas may also have knowledge of performance concerns through line manager reporting or analysis of employment data, such as unexplained absences or unplanned leave. These performance concerns could be indicators of other personal issues that can lead to security concerns, for example alcohol or drug abuse, or financial difficulties.

The relationship between performance issues and security concerns is complex. It is important that entities do not misuse the security clearance process to address performance issues (e.g. referring security concerns to the Authorised Vetting Agency in the hope that a security clearance may be withdrawn).

Performance management processes or investigations do not preclude entities from providing the Authorised Vetting Agency with information about security relevant performance issues.

Recommended Approaches

- Develop clear processes for line managers to provide this information to security practitioners responsible for entity personnel security, and for the security practitioners to provide the information to the Authorised Vetting Agency.
- Provide line managers with guidance on identifying behaviours of concern and engaging in effective conversations about personnel security within the context of performance management.
    - Examples include confirming compliance with mandatory security awareness training, and ensuring understanding of reportable incidents and the contact reporting scheme.
- It is also important to identify gaps in knowledge about security, particularly where specialist knowledge or training is required to address entity-specific risks or in relation to compartmental briefings.
- The Sponsoring Entity should develop procedures and provide guidance for human resources areas to support information sharing arrangements and assist with identifying and communicating information.

21.3.1.3. Periodic Employment Suitability Checks

Pre-employment screening provides the foundation of good personnel security and reduces the risk of an insider harming business operations.

Pre-employment screening checks can be repeated periodically over the course of a person's employment to inform an assessment of ongoing suitability.

Table 50 describes a range of recommended periodic employment suitability checks.

Table 50: Periodic Employment Suitability Checks

Check Type	Description
Updating personal particulars	Personnel may be asked to periodically update their personal particulars. This could include: • updating residential address history • updating any qualifications • updating employment history for contractors. It may be useful to verify changes to personal particulars through independent sources, including the Document Verification Service, if there are changes to Australian-issued primary identification documents.
Confirming adherence to, or completion of, engagement conditions	Where conditions have been placed on an initial or continuing engagement (e.g. gaining Australian citizenship), confirm those conditions have been met within specified timeframes.
National police check	If police checks are conducted less frequently than every 10 years, convictions under the Spent Convictions Scheme may not be included. A police records check at least every 10 years is recommended; the frequency may be increased for high-risk positions or personnel. The Spent Convictions Scheme applies to spent convictions where a waiting period has passed and the individual in question has not re-offended. The conditions that apply to convictions for a Commonwealth, state, territory or foreign offence are: • it has been 10 years from the date of the conviction (or 5 years for juvenile offenders) • the individual was not sentenced to imprisonment for more than 30 months • the individual has not re-offended during the 10 year (5 years for juvenile offenders) waiting period • a statutory or regulatory exclusion does not apply. The scheme also protects convictions that have been set aside or pardoned under Part VIIC of the *Crimes Act 1914*. An individual whose conviction is protected does not have to disclose the conviction to any person, including a Commonwealth authority.
Credit history check	Where an entity's risk assessment deems that it requires assurance of a person's financial situation, periodic financial screening (including a credit history check) may provide indicators of financial stressors.
Conflict of interest declaration	APS employees have an obligation under section 13 of the *Public Service Act 1999* to disclose and take reasonable steps to avoid actual or perceived conflicts of interest. Reconfirming with personnel that any changes in their circumstances have not resulted in any actual or perceived conflict of interest is recommended. For information, see the APSC advice on Declarations of interest.
Confidentiality agreement	Periodic completion of confidentiality or non-disclosure agreements helps remind personnel of their ongoing confidentiality obligations.
Other entity-specific checks	Personnel who are in positions subject to entity-specific pre-employment checks may have these checks periodically repeated. Examples of entity-specific checks include drug and alcohol testing, financial probity checks and psychological assessments. For information, see APSC's Conditions of engagement.

Recommended Approach

- ✔ Entities should determine the frequency of periodic employment suitability checks based on the entity's risk profile as well as specific risks associated with the position, any associated enabling legislation and the entity's operating environment.

21.3.1.4. Contact Reporting Obligations

Reporting suspicious, unusual or persistent contacts and incidents, as well as contact with foreign and Australian nationals who are seeking information that they do not need-to-know, is one means to address the enduring threat that espionage poses to the Australian Government.

Contact reporting obligations are set out in PSPF Release 2024 (Table 2) and ASIO's Contact Reporting guidance (available on GovTEAMS).

These reporting obligations are relevant when assessing ongoing suitability of personnel. Reports of suspicious, ongoing, unusual or persistent contacts may inform an entity's risk assessment in relation to an individual, a position or a work area. Non-compliance with contact reporting obligations is a security concern.

PSPF Requirement 0168 mandates that entities conduct annual security checks for all security cleared personnel, which includes the responsibility for Sponsoring Entities to share information about suspicious, unusual or persistent contacts from foreign and Australian nationals with personnel, with the Authorised Vetting Agency, in addition to forwarding reports to ASIO.

21.3.1.5. Security Incident Reporting and Follow Up

PSPF Requirement 0026 mandates that entities establish procedures for managing security incidents.

Managing security incidents and investigations helps monitor security performance, identify inadequacies in security procedures and detect security risks in order to implement appropriate treatments. At the individual level, a history of security incidents (regardless of their individual scale or significance) may raise questions about a clearance holder's suitability to retain access to Australian Government resources.

PSPF Requirement 0177 mandates that Sponsoring Entities share with Authorised Vetting Agencies any security concerns about a security clearance holder.

21.3.1.6. Collecting and Assessing Information on Changes in Circumstance

Reporting changes in circumstance helps entities assess personnel security risk based on current and relevant information. Early identification of changes in risk profiles can prevent smaller issues from becoming larger problems.

At the individual level, this means encouraging and enabling self-reporting of changes in circumstance by personnel. At the entity level, this means having effective procedures to collect, assess and manage reported changes in circumstances.

Authorised Vetting Agencies grant security clearances after careful consideration of the whole-of-person assessment at the time of granting the clearance. However, as circumstances change over time, this may affect ongoing eligibility and suitability of a person to hold a clearance. Changes in circumstances may:

- increase a person's vulnerability to coercion
- lead to deliberate breaches of security, fraud or corruption
- be used by foreign governments, commercial organisations, issue-motivated groups, criminal organisations or others to induce personnel into providing information or goods belonging to the government.

Table 51 provides guidance on entity responsibilities for assessing and managing changes in circumstances.

Table 51: Guidance on Reporting Changes in Circumstance

Check Type	Description
What changes in circumstance to report	Changes in circumstance are reportable where there are: • changes of name/identity (gender) • changes in significant relationships • changes in address or share-housing arrangements • entering into, or ceasing, a relationship (marriage, civil union or de facto) • changes in citizenship or nationality • changes in financial circumstances • changes in health or medical circumstances • changes in criminal history, police involvement and association with criminal activity • involvement or association with any group, society or organisation • disciplinary actions • drug or alcohol problems • residence in, or visits to, foreign countries • relatives residing in foreign countries • suspicious, persistent or unusual contacts • any other significant changes in circumstance. This list is not exhaustive. If personnel are uncertain whether the information is relevant, report it to the line manager, CSO or a security practitioner responsible for personnel security.
How to report changes in circumstances	Entities should: • make clear the process and responsible area within their entity where clearance subjects report any change in circumstances • require clearance holders to report all changes in circumstances to the identified area • require line managers to report all changes in circumstances relating to their clearance holder personnel, regardless of whether they believe changes have been notified by the clearance subject • encourage all staff to advise line managers of significant changes in circumstances (noting this may not always be appropriate). Entities must provide security awareness training and establish procedures for managing security incidents. Security awareness training should cover entity procedures to report changes in circumstance in a manner that enables, encourages and facilitates timely reporting.
Who reports changes in circumstances	Where personnel fall into more than one listed category, report in accordance with all applicable categories: • security clearance holders report changes in their circumstances • line managers and contract managers report any concerns with personnel they manage • human resources areas report any employment-related concerns or investigations, including those related to breaches of the Code of Conduct • personnel report concerns about other individuals, including their manager, where it may affect the security of the entity.
What to do with information on changes in circumstances	When an entity is advised about an individual's change in circumstances, the entity considers that information for the purposes of assessing and managing the ongoing suitability of that individual, and shares information of security concern, where appropriate. Entities share all reports of changes in circumstances relating to clearance holders with the relevant Authorised Vetting Agency, which may initiate actions in relation to the

Check Type	Description
	person's security clearance. The Authorised Vetting Agency will notify the Sponsoring Entity to allow it to manage any associated risks. Entities assess all reports of changes in circumstances to identify whether there are any security concerns for the entity, and respond to those concerns in accordance with entity procedure. If there are potential security concerns as a result of changes in circumstances, there are different avenues that can be pursued by the Sponsoring Entity. These include: • security investigations • code-of-conduct investigations • criminal investigations. Where an allegation of security concern is received, an investigation by the Sponsoring Entity or the Authorised Vetting Agency may validate the report. It is important that entities do not prejudice the person in question, as some claims can be malicious. For information, see the Australian Privacy Principle 10 – quality of personal information. Where a Sponsoring Entity's investigation brings to light any additional information of security concern, this information be shared with the relevant Authorised Vetting Agency.

21.3.1.7. Monitoring Compliance with Conditional Security Clearances

Where there are ongoing concerns about a clearance subject's eligibility or suitability to hold a security clearance, but they are not sufficient to deny the clearance, an Authorised Vetting Agency may, after consultation with the Sponsoring Entity, recommend clearance conditions to mitigate these concerns in accordance with PSPF Requirement 0158. If agreed by the Sponsoring Entity and clearance subject, the Authorised Vetting Agency may issue a conditional clearance.

PSPF Requirement 0165 mandates that Sponsoring Entities monitor security clearance holders granted a conditional security clearance to ensure compliance with the conditions and manage any related risks. Sponsoring Entities are also required to report any non-compliance to the Authorised Vetting Agency. Some conditions may also specify a reporting regime to the Authorised Vetting Agency to ensure compliance.

PSPF Requirement 0167 mandates that Authorised Vetting Agencies share information of security concern about security clearance holders with Sponsoring Entities. In the case of conditional security clearance holders, this information is essential for Sponsoring Entities to effectively identify and manage any risks related to the conditional security clearance.

21.3.1.8. Clearance maintenance for personnel on secondment or temporary assignment

In accordance with PSPF Requirement 0177, PSPF Requirement 0178 and PSPF Requirement 0179, the losing and gaining entities are required to share information of security concern about the clearance holder with each other and with the relevant Authorised Vetting Agency. This includes concerns identified after the secondment or temporary assignment concludes.

Recommended Approach

- Entities should explicitly agree on security clearance arrangements for personnel who are seconded, or are on temporary assignment, before the secondment or assignment commences.
- It may be appropriate to transfer sponsorship of the security clearance to the receiving entity for the period of the secondment or assignment (depending on the length of time and the level of access still required to the losing entity's resources).

21.3.1.9. Ongoing assessment and management of TOP SECRET-Privileged Access clearances

The TOP SECRET-Privileged Access Standard includes additional specific requirements for assessing and managing the ongoing suitability of TOP SECRET-Privileged Access security clearance holders.

The Standard is a classified document that is only available to qualified practitioners conducting TOP SECRET-Privileged Access vetting, psychological assessments or insider threat management activities in Authorised Vetting Agencies or Sponsoring Entities (referred to as TOP SECRET-Privileged Access practitioners).

21.3.1.9.1. Sponsoring Entities

In accordance with PSPF Requirement 0163, sponsoring agencies are to implement specific requirements in the TOP SECRET-Privileged Access Standard to assess and manage the ongoing suitability of TOP SECRET-Privileged Access security clearance holders.

This includes, but is not limited to, conducting annual security checks, facilitating contact reporting, collecting and assessing information of security concern (including changes of circumstances), monitoring compliance with conditional security clearances and reviewing eligibility waivers at least annually.

The TOP SECRET-Privileged Access Standard requires all entities that manage TOP SECRET-Privileged Access 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 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.

21.3.2 Share Information of Concern

The PSPF Release 2024 mandates several requirements on the sharing of information of security concern during a clearance subject's vetting process, outlined below:

- PSPF Requirement 0167 mandates that the Sponsoring Entity shares relevant information of security concern, where appropriate.
- PSPF Requirement 0177 mandates that the Sponsoring Entity shares relevant information of security concern, where appropriate with the Authorised Vetting Agency.
- PSPF Requirement 0177 mandates that entities share all information of security concern. The assessment of whether information is of security concern can only be made by the entity assessing that concern. Therefore, all information pertaining to personnel is shared between Sponsoring Entities and Authorised Vetting Agencies so that they can determine whether it is relevant.

See PSPF Guidelines Section 19.6 for further guidance.

21.3.3 Annual Security Checks

PSPF Requirement 0168 mandates that entities conduct an annual security check with all security cleared personnel. 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, and 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
- the person's workplace behaviours to identify behaviours of concern.

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.

Line managers are well placed to conduct an annual security check as they are likely to have the best knowledge of their personnel's behaviour. 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.

PSPF Requirement 0177 mandates that Sponsoring Entities share with Authorised Vetting Agencies any security concerns about a security clearance holder identified during annual security checks, in addition to reporting any changes in circumstances, security incidents, and suspicious, ongoing, unusual or persistent contact reports as they occur.

For personnel holding a TOP SECRET-Privileged Access security clearance, the Sponsoring Entity is required to provide the relevant Authorised Vetting Agency with information from the annual security check to inform the annual clearance review as set out in the TOP SECRET-Privileged Access Standard.

21.3.4 Review Eligibility Waivers

PSPF Requirement 0169 mandates that Sponsoring Entities 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 clearances 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.

21.3.5 Implement TS-PA Standard

Sponsoring agencies are to implement specific requirements in the TOP SECRET-Privileged Access 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), and
- 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. See PSPF Guidelines Section 7.3 for guidance on insider threat programs.

21.4 Clearance Holder Maintentance Obligations

Holders of an Australian Government security clearance must meet obligations in order to retain the 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 that meets the requirements of holding 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 entity's security unit or Authorised Vetting Agency
- report suspicious, unusual or persistent contacts and incidents (contact reporting) with 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 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.

Personnel who hold a TOP SECRET-Privileged Access security clearance are provided with a copy of the annex to the TOP SECRET Privileged Access Standard that outlines their obligations for maintaining their security clearance, which include reporting requirements.

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 again considering the required character traits. These traits are:

- for Baseline, Negative Vetting 1, Negative Vetting 2 and Positive Vetting security clearances, the clearance holder's integrity in accordance with the Personnel Security Adjudicative Standard (PSPF Requirement 0172).
- for TOP SECRET-Privileged Access security clearances, the clearance holder's trustworthiness and commitment to Australia in accordance with the TOP SECRET-Privileged Access Standard (PSPF Requirement 0173)

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.

In accordance with PSPF Requirement 0171 and PSPF Requirement 0172 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.

21.5.1 Revalidation Timeframes

Authorised Vetting Agencies are to commence the revalidation process sufficiently before the due date so that the security clearance does not lapse. Where new security concerns are identified during the revalidation process, the allowed time may not be sufficient.

Authorised Vetting Agencies are required to share information of security concern about security clearance holders with Sponsoring Entities including allowing the Sponsoring Entity to suspend or limit the clearance holder's access to Australian Government resources until the concerns are resolved.

The recommended timeframes for commencing the revalidation process, prior to the expiry date of a security clearance, for each security clearance level is listed in Table 52 below.

Table 52: Levels of Identity Assurance for Security Clearances

Security Clearance Level	Recommended Commencement of Revalidation Process
Baseline	1-3 months prior to the expiry date of the security clearance
Negative Vetting 1	3-6 months prior to the expiry date of the security clearance
Negative Vetting 2	9-12 months prior to the expiry date of the security clearance
Positive Vetting	12-18 months prior to the expiry date of the security clearance
TS-PA	12 months prior to the expiry date of the security clearance

Recommended Approach

- Authorised Vetting Agencies contact the Sponsoring Entity before commencing the revalidation of a security clearance to confirm the continuing security clearance requirements.
- Entities identify and record positions that require a security clearance and the level of clearance required.
- Entities ensure that each person working in an identified position have a valid security clearance issued by an Authorised Vetting Agency.
- This responsibility extends to where a clearance holder's duties or role has changed. If a higher level clearance is required, a new clearance process will be necessary.

21.6 Information Sharing on Security Clearances

PSPF Requirement 0167 mandates that entities share information of concern, where appropriate. This includes sharing information between line managers, human resources areas and security practitioners as well as sharing information between Sponsoring Entities and Authorised Vetting Agencies.

This requirement is relevant to information sharing in relation to transfers of personnel, including temporary and permanent transfers within entities and to other entities. Information covered by this requirement includes all information relevant to an individual's ongoing eligibility and suitability for employment or to hold an Australian

Government security clearance. Information sharing may be limited by legislation, including the Australian Privacy Principles and an entity's enabling legislation.

21.6.1.1. Consent

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 Authorised Vetting Agencies for the purposes of assessing their ongoing eligibility and suitability.

In some circumstances, there is a reasonable expectation that personal information will be shared, such as when an individual's information is crucial to rectify a security incident.

Recommended Approach

- Consent should be 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.

21.6.2 Security Culture and Information Sharing

A well-developed culture of security encourages information sharing by personnel about the risks to themselves and their colleagues. Information sharing is dependent on an entity's aim to help manage concerns with their personnel before they escalate into an incident.

While the focus is on prevention, entities are encouraged to have a clear, published and consistently enforced security regime that investigates and penalises inappropriate conduct.

21.7 International Travel

Negative Vetting 2, Positive Vetting and TOP SECRET-Privileged Access security clearances have specific obligations in relation to international travel.

PSPF Requirement 0180 mandates that security clearances holders must receive appropriate departmental travel briefings when undertaking international personal and work 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 TOP SECRET-Privileged Access 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.

Recommended Approach

- Negative Vetting 1 security clearance holders receive appropriate departmental travel briefings when undertaking international personal and work travel.

22 Separation

Entities are required to develop and use procedures that ensure relevant security policy or legislative obligations are met. 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.

Entities should ensure that separating personnel have their access to Australian Government information and resources withdrawn, and are informed of any ongoing security obligations.

PSPF Requirement 0021 requires entities to develop and use procedures that ensure relevant security policy or legislative obligations are met.

Recommended Approach

- Procedures for managing personnel security during separation are established and tailored to the level of access to security classified information and resources, and the entity's assessment of the security risk.

See PSPF Release 2024 (Section 20.3) for information on the separation of ministerial staff employed under Part III on the *Members of Parliament (Staff) Act 1984.*

22.1 Debriefing Procedures

Prior to separation, PSPF Requirement 0182 mandates that entities debrief separating personnel who have access to security classified information. This may include caveated and compartmented information where additional briefing requirements apply. See the Australian Government Security Caveat Standard (available on GovTEAMS).

PSPF Requirement 0182 also mandates that entities advise separating personnel of their continuing obligations under the *Criminal Code Act 1995* and other relevant legislation, and obtain the person's acknowledgement of these obligations.

This acknowledgement helps safeguard Australian Government information and resources and limits the potential for the integrity, availability and confidentiality of security classified information to be compromised.

22.1.1 Sharing Relevant Information

In accordance with PSPF Requirement 0181, the entity's CSO, CISO or relevant security practitioner, is notified of any proposed cessations of employment resulting from misconduct (e.g. termination for cause or resignations following concerning conduct).

If separation is the result of an incident (or if an incident is uncovered during the separation process), advise other affected entities if their interests or security arrangements could be affected.

Recommended Approach

- Risk assessment informs any security measures for personnel whose employment has been terminated, including security measures for high-risk personnel that may include immediate suspension of duties, immediate removal of all access to entity systems and facilities and escorting the person from the premises.

22.1.2 Sharing Information on Transfer

In accordance with PSPF Requirement 0183, when personnel are transferring to another entity, the losing entity must provide the gaining entity with relevant security information.

Relevant security information includes the outcome of pre-employment screening checks and any periodic employment suitability checks, as well as concerns that were mitigated as part of the employment screening process.

22.1.3 Security Concerns and Risks

PSPF Requirement 0184 mandates that entities identify and report any security concerns to ASIO (security is defined in the in thehttps://www.legislation.gov.au/Latest/C2016C01133 ASIO Act). An example of where this may be particularly relevant is when separating personnel do not adhere to requirements of this policy (e.g. those departing without having a security debrief).

PSPF Requirement 0184 mandates that entities identify and report any security concerns to ASIO (security is defined in the in the ASIO Act).

This is particularly relevant when separating personnel do not adhere to requirements of this policy (e.g. those departing without having a security debrief).

Recommended Approach

- Entities provide personnel with an opportunity to confidentially express any security concerns relating to procedures or colleagues prior to separation.

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.

Table 53 provides an example of actions for entities to consider prior to, and on separation of, personnel.

Table 53: Processes for Withdrawing Access (Prior to, and on, Separation or Transfer of Personnel)

Stage	Actions
Prior to separation	• recover IT equipment or physical assets that are issued to personnel, in particular, any portable devices, and where entities allow the transfer of ownership of IT equipment to separating personnel, or where entities allow the use of personal devices for work purposes entities should:

Stage	Actions
	○ archive any business related documents in accordance with entity records management procedures ○ remove entity information ○ remove all entity software applications, and ○ if necessary, erase the entire device's hardware • recover any corporate credit cards • recover any hardcopy material (both originals and copies).
On separation	• disable access to the IT systems, including but not limited to email, telephone voicemail, Citrix, dropbox and cloud accounts • revoke physical access to facilities and retrieve keys and access cards • change any combinations for locks (e.g. doors, safes or security containers) that the person had access to.

Recommended Approach

✔ Entities should consider the sequencing of withdrawal of access to resources.

22.2.1 Separation Risk Assessment

PSPF Requirement 0185 mandates that entities undertake a risk assessment to identify any security implications where personnel depart without undertaking required separation procedures. This could include personnel who suffer injury or illness and cannot continue working, personnel who separate while on leave, or personnel who refuse to undergo separation processes.

For personnel taking extended leave, the risk assessment might consider the purpose of the leave, any travel plans, the degree of ongoing contact between the entity and the individual during the leave and whether it is likely the individual may decide not to return from leave.

This assessment can inform the entity's decision on whether to apply separation procedures prior to the commencement of extended leave.

22.3 Post-Separation Security Clearance Actions

Security clearance actions only apply to personnel that hold a security clearance and take place after separation or transfer.

PSPF Requirement 0187 and PSPF Requirement 0188 set out the roles and responsibilities of Sponsoring Entities and Authorised Vetting Agencies for the separation of security cleared personnel.

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.

22.3.1 Managing and Recording Security Clearance Status

In accordance with PSPF Requirement 0188, Authorised Vetting Agencies manage and record changes in separating personnel's security clearance status, including where there is a change of sponsorship.

A security clearance can be sponsored by an Australian Government entity (or otherwise authorised by the Australian Government, for example, under an agreement with the states and territories) and can only be sponsored by one entity at a time. Authorised Vetting Agencies may allow entities to register their interest in the clearance (i.e. contractors working for more than one entity, or secondees where both the home and host entities have an interest).

22.3.2 Personal Security File

PSPF Requirement 0188 mandates that Authorised Vetting Agencies transfer personal security files where a clearance subject transfers to an entity covered by a different Authorised Vetting Agency (where enabling legislation allows). Table 54 identifies recommended actions to take in such cases.

Table 54: Recommended Personal Security File Actions

Stage	Actions
Prior to separation	• recover IT equipment or physical assets that are issued to personnel, in particular, any portable devices • recover any corporate credit cards • recover any hardcopy material (both originals and copies).
Permanent transfer	**Actions for the gaining Sponsoring Entity** Before personal security file actions commence, the gaining Sponsoring Entity: • identifies the level of security clearance required and whether the clearance subject has previously held a security clearance (including the entity that sponsored the previous clearance) • obtains the clearance holder's consent to share information where a current or previous clearance is identified • requests permanent transfer of sponsorship of the security clearance. This will trigger the Authorised Vetting Agency to commence permanent transfer of the personal security file. **Actions for the gaining Authorised Vetting Agency** Once it has received a request for the permanent transfer of a security clearance from the gaining Sponsoring Entity, the gaining Authorised Vetting Agency: • requests the personal security file from the losing Authorised Vetting Agency o Some entities have legal restrictions on the transfer of personal security files. For example, the Department of Defence cannot transfer the personal security files of current and former Regular or Reserve Australian Defence Force personnel and ASIO can only transfer personal security files to other AIC entities. ASIO can only provide a statement of clearance to other vetting agencies. o Psychological assessments may only be transferred to another appropriately qualified psychologist and only with the specific consent of the clearance holder. • confirms the information in the personal security file meets the requirements for the requested level of security clearance, or commences a new vetting process if the Sponsoring Entity requires a clearance that is higher than the clearance held • identifies and addresses concerns or anomalies in the personal security file at the time of transfer, including determining whether the concerns or anomalies warrant a review for cause • confirm the transfer of the personal security file with the Sponsoring Entity, including if further actions will be undertaken before the transfer of sponsorship can be finalised (i.e. sharing any concerns or conducting a review for cause). **Actions for the losing Authorised Vetting Agency:**

Stage	Actions
	The losing Authorised Vetting Agency: • facilitates transfer of the personal security file as soon as practicable, following receipt of request from the gaining Authorised Vetting Agency o In some instances it may not be possible to transfer personal security files immediately. This includes where personnel are still employed by the losing entity, are under investigation for a security breach or violation, are being revalidated, or are undergoing a review for cause. • seeks consent from clearance subjects prior to transferring and sharing personal security files.
Temporary transfer	Only transfer personal security files if necessary, for example: • the position in the gaining Sponsoring Entity requires a higher security clearance • the clearance expires during the transfer or secondment period.

Where a personal security file contains a National Police Check subject to no exclusions under the Commonwealth spent convictions scheme, the scheme requires entities ensure any previous recorded convictions are not spent and reference to any convictions that are spent are removed. For information, see the Privacy fact sheet 41: Commonwealth spent convictions scheme.

Transferred personal security files may include information that has been previously collected (e.g. personal information or copies of supporting information).

Recommended Approach

- If the original National Police Check is not shared (as a result of Commonwealth spent convictions scheme requirements), the gaining Authorised Vetting Agency requests a new National Police Check on transfer of the personal security file.
- Where there are concerns transferring personal security files, Authorised Vetting Agencies will advise the Sponsoring Entity. The Sponsoring Entity can then make a risk-based decision on providing or continuing access to Australian Government resources.
- The gaining Authorised Vetting Agency should not request this information again, unless there are concerns about the authenticity of the documents originally supplied.
- If electronic packs are used, information may be regathered electronically to populate the electronic record; this occurs at the next revalidation or review of the security clearance.

22.3.3 Temporary Transfer or Secondment

Entity processes for the sponsorship of security clearances (including associated responsibilities for assessment and management of ongoing suitability for clearance holders on temporary transfer or secondment) need to be:

- flexible to account for the diversity of timeframes and arrangements applicable to secondment and other temporary transfers, and
- negotiated between the home entity and host entity on a case-by-case basis.

Recommended Approaches

- The losing Sponsoring Entity (the home entity), in consultation with the gaining Sponsoring Entity (the host entity) determine whether to treat a temporary transfer or secondment as a separation for the purpose of security clearance sponsorship. Relevant factors to consider include:
    - the duration of the transfer or secondment and the level of access personnel will require to the home entity and host entity resources during the transfer or secondment

- whether the host entity requires a security clearance for the position at the same, higher or lower level than the home entity, and
- whether both entities use the same Authorised Vetting Agency and if there is a need to transfer the clearance holder's personal security file.

- If the host entity requires a higher level of clearance or the clearance expires during the period of the temporary transfer, the host entity's Authorised Vetting Agency is responsible for the upgrade of the clearance.

22.3.3.1. Extended leave

The definition of separating personnel includes those taking extended leave and personnel on leave without pay. As such, the personnel security requirements of this policy apply, unless a risk assessment determines this is not necessary.

Generally 'extended' leave is defined as 3-6 months or longer, however entities may elect to define a shorter period of time for extended leave, for example 3 months. Where a clearance holder does not maintain their security clearance for a period greater than 6 months due to long-term absence from their role, the security clearance is considered inactive.

Entities are encouraged to balance the security risks with other desired human resource outcomes when applying the separation procedures to personnel on extended leave. For example, the entity may wish to allow personnel on maternity or paternity leave to maintain ongoing access to the entity's buildings, but suspend access to security classified information and resources (including administrative accounts) for the period of leave.

Recommended Approaches

- Entities advise the Authorised Vetting Agency to change clearances to inactive for personnel on extended absences based on their risk assessment. When clearance subjects return to work, the Authorised Vetting Agency can make the clearance active, if requested, after undertaking appropriate vetting updates.
- Entities include personnel security guidance on the following in their human resources or leave-related procedures:
  - notifying relevant security practitioners in advance of personnel commencing extended leave, as well as completing risk assessments if required
  - considering and managing security issues before extended leave is approved, particularly if it is assessed as likely that personnel may decide not to return (entities are encouraged to resolve any security issues before the leave commences)
  - reminding personnel on extended leave of their ongoing confidentiality obligations
  - briefing personnel travelling overseas of their responsibilities, including the requirement to report suspicious, unusual or persistent contacts, as well as contact with foreign nationals that becomes ongoing, and
  - advising the Authorised Vetting Agency when a security clearance holder is taking extended leave and requesting the clearance status be changed to inactive
- Ensuring recommencement procedures include changing the status of the security clearance and noting that the Authorised Vetting Agency may need to undertake vetting updates.

Part Six

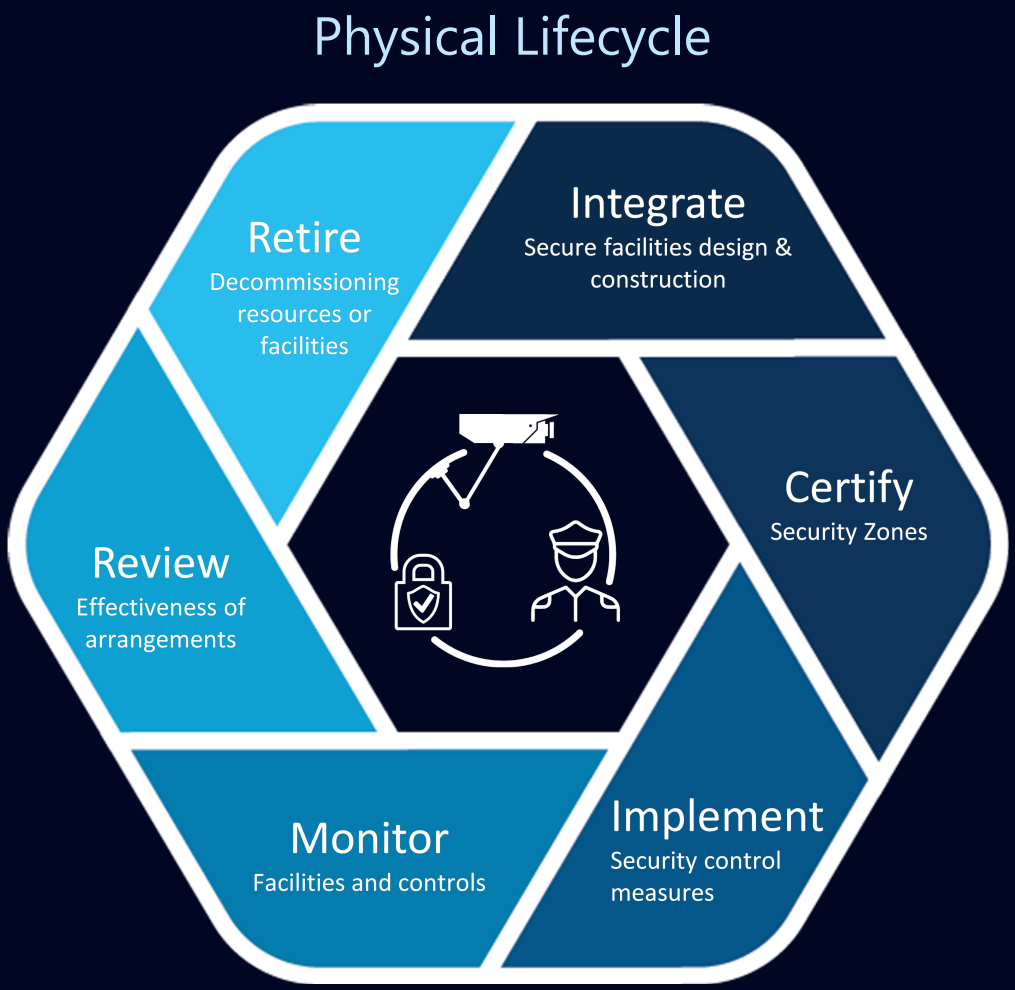
Physical

Physical Security Lifecycle

Security Zones

Physical Security Measures and Controls

Event Security



23 Physical Security Lifecycle

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 resources secured by those facilities.

PSPF Requirement 0189 mandates that protective security is integrated in the process of planning, selecting, designing and modifying entity facilities for the protection of people, information and physical resources. This means protective security must be integrated during all stages of the physical security lifecycle, including the planning, selection, designing, approving, operating, modifying, reviewing and retiring of entity facilities.

23.1 Plan Entity Facilities

Site securing 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.

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.

Security risks during business hours may be significantly different to those experienced out-of-hours. For example:

- Work hours: increased risks from public and client contact, as well as from insider threats.
- During Out-of-hours: external threats, such as break and enters.

23.1.1 Facility Security Plan

PSPF Requirement 0190 mandates that entities develop a facility security plan for new facilities, facilities under construction or major refurbishments of existing facilities to assess the associated security risks.

The major concerns are the location and nature of the site, the ownership or tenancy of the site (sole or shared, including multiple entities sharing the same space) and the 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 and other security classified discussions and meetings.

Loss of power supply can have a significant effect on the security of entity resources (for example loss of power could affect the operation of access control systems and security alarm systems) and is one of a number of considerations when developing the 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 and other security classified discussions and meetings
- other resources that will be on the site, and
- protective security measures required for:
  - the site as a whole (holistic view of the whole site)
  - specific discrete areas within the facility (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 may be more prevalent out-of-hours.

23.1.2 Facility Site Selection

Site selection is an important part of planning and needs to factor 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.

Security-in-depth is a multi-layered system in which security measures combine to make it difficult for an intruder or authorised personnel to gain unauthorised access.

PSPF Requirement 0191 requires decisions on the locations of entity facilities to be informed by considering the site selection factors detailed in PSPF Release 2024 (Table 35).

Entities should situate technology facilities within Security Zones commensurate with the security classification of the information accessed, stored, processed or transmitted from within the facility and should ensure their construction meets the requirements set out within the ASIO Technical Notes. Entities must ensure that all TOP SECRET information technology facilities are in compartments within an accredited Zone Five area and comply with ASIO Technical Note 5/12 (Annex A) – Compartments within Zone Five areas. See PSPF Guidelines Section 13.6 for guidance on Technology Facilities.

Recommended Approach

- The CSO and security practitioners should be involved in 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.

23.2 Design and Modify Entity Facilities

PSPF Requirement 0192 mandates that 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, to protect the security classified information, resources or activities that will be processed, stored or communicated in that area.

Facilities should be designed or modified using successive layers of physical security to:

- 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.

For new constructions or for significant modifications to facilities, entities must consider the:

- protective security measures as early as possible, preferably during the concept and design stages
- siting within a facility of entity functions that need security measures so that these locations can be constructed or modified to provide appropriate protection, and
- suitability of construction methods and materials to give the protections needed.

Where an entity's security risk assessment identifies a viable risk, entities should employ additional security mitigations for the protection of personnel and assets, other than security classified assets. These protective security mitigations are especially related to overt and covert attacks from foreign intelligence services and malicious insiders.

Recommended Approach

- ✔ Consider the location of vulnerable areas, such as mailroom and parcel delivery areas, that may be exposed to threats such as explosive devices, chemical, radiological and biological attacks, and apply appropriate physical mitigations (e.g. mail-screening devices, a stand-alone delivery area or using a commercial mail receiving area and sorting service).

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)[18].

Entities may include additional building elements to address specific risks identified in their risk assessment where building hardening[19] 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).

PSPF Requirement 0193 mandates that entities must construct facilities in accordance with the applicable ASIO Technical Notes to protect against the highest risk level in accordance with the entity security risk assessment.

[18] Various state and territory Acts and Regulations set out the legal framework for design and construction of buildings in accordance with the BCA.
[19] Building hardening is the process where a building is made a more difficult or less attractive target.

The ASIO Technical Notes detail the protective security mitigations to maintain the confidentiality and integrity of security classified information and resources. These protective security mitigations are especially related to overt and covert attacks from foreign intelligence services and malicious insiders.

The ASIO Technical Notes are available to Australian Government security personnel on GovTEAMS.

PSPF Requirement 0194 mandates that for facilities that store security classified information and resources, entities must construct facilities in accordance with the applicable ASIO Technical notes, outlined in Table 55.

Table 55: ASIO Technical Notes applicable to Security Zones

Security Zone	Relevant ASIO Technical Notes
Zones Two	ASIO Technical Note 1/15 – Physical Security Zones
Zone Three	ASIO Technical Note 1/15 – Physical Security Zones
Zone Four	ASIO Technical Note 1/15 – Physical Security Zones
Zone Five	ASIO Technical Note 5/12 – Physical Security Zones (TOP SECRET) area
Compartments within Zone Five areas	Annex A – ASIO Technical Note 5/12 – Compartments within Zone Five areas

23.4 Operate and Maintain Entity Facilities

Entities must ensure facilities remain fit-for-purpose to meet their operating environment by ensuring the protective security measures are contemporary with evolving security threats and vulnerabilities.

PSPF Requirement 0195 mandates that entities operate and main facilities in accordance with Security Zones and Physical Security Measures and Controls. See PSPF Guidelines Section 25 for detailed guidance.

Entities should establish procedures that promote awareness of the requirements to protect information and resources from compromise and assist entity personnel to secure all files, documents, security classified material and other official information in their custody. See PSPF Guidelines Section 9.3 for further information.

23.4.1 Review or Retire Entity Facilities

Entities should undertake regular reviews to ensure your security measures remain fit-for-purpose by proactive identifying changes in the use of their facilities, their organisation or the threat environment.

When a facility is no longer needed, develop a plan for retiring, destroying, redeploying or disposing of the facilities and the information and resources located in that facility. Ensure the plan accounts for information or equipment to be stored securely while it awaits destruction, disposal or redeployment and when it is being transported to a suitable destruction facility.

See PSPF Guidelines Section 9.3—Minimum Protections and Handling Requirements, Section 11—Information Disposal and Section 13.7—Technology Asset Disposal.

23.5 International Entity Facilities (including Missions and Posts)

All Australian Government international entity facilities, including missions, posts, embassies and consulates (including those managed by DFAT), are required to meet the PSPF requirements and be included in the managing entity's annual protective security report.

The managing entity of each mission / post is responsible for the implementation the PSPF to ensure appropriate physical, technical, information and personnel security procedures, measures and standards, and for coordinating business continuity and contingency planning at each mission/post.

Generally, DFAT is the managing entity responsible for all aspects of security policy for international entity facilities, however, other entities can assume this responsibility where DFAT is not represented.

DFAT is responsible for all Australian missions and staff attached to DFAT-managed missions.

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.

PSPF Requirement 0195 mandates that entities operate and main facilities in accordance with Security Zones and Physical Security Measures and Controls. See PSPF Guidelines Section 25 for detailed guidance.

The PSPF Release 2024 (Table 37) provides broad descriptions of each zone for the protection of security classified information and resources, including examples of where the zones might be used and the personnel security clearance requirements for each zone.

24.1.1 Secure Areas in International Entity Facilities (including Missions and Posts)

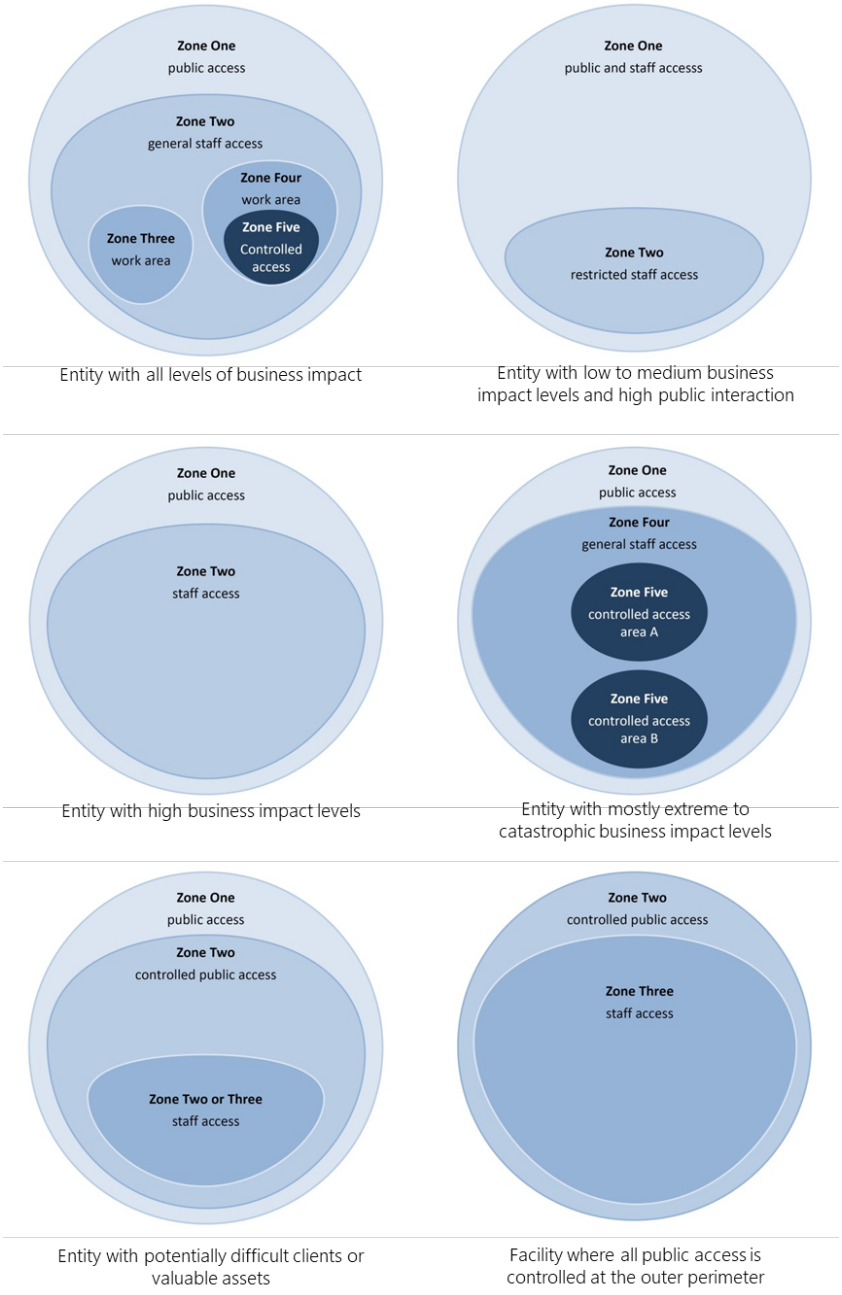
The location and threat environment of some Australian Government international entity facilities (including missions and posts) necessitate more stringent protective security arrangements than entity facilities located in Australia. DFAT-managed overseas entity facilities use different terminology for '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 PSPF Release 2024 (Table 38).

24.1.2 Layering Security Zones

Entities should layer zones, working in from Zone One public access areas, and increasing the level of protection with each new zone. Multiple layers are the 'delay' design feature to provide more time to detect unauthorised entry and respond before resources are compromised.

Figure 13 provides examples of how layering of zones can be implemented for different purposes. In some instances it may not be possible for higher zones to be fully located within lower zones and entities may need to strengthen higher zone areas.

Figure 13: Example Layering of Security Zones



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 by establishing the zone's compliance with the minimum physical security requirements to the satisfaction of the relevant certification authority

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.

PSPF Requirement 198 mandates that Zones One to Four 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. PSPF Requirement 199 mandates that Sensitive Compartmented Information Facility areas used to secure and access TOP SECRET systems and security classified compartmented information are accredited by ASD before they are used operationally.

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.

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, sensitive compartmented information (SCI) or aggregated information where the aggregation of information increases its business impact level to catastrophic, ASIO-T4 is the Certification Authority.

PSPF Release 2024 (Table 39) outlines the certification authorised for security zones.

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.

ASD must accredit Zone Five facilities used to secure and access sensitive compartmented information. As well as Sensitive Compartmented Information Facility (SCIF) accreditation ASD is responsible for management of all SCIFs in Australia.

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; for:
  - Zone Two: ten (10) years
  - Zones Three to Five: five (5) years
- 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.

An entity's CSO or delegated security practitioner should seek advice from ASIO-T4 for recertification of Zone Fives and SCIFs.

25 Physical Security Measures and Controls

PSPF Release 2024 describes the physical protections required to safeguard people (consistent with the requirements of the *Work Health and Safety Act 2011*), information and resources (including IT equipment) to minimise or remove security risk.

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
- the compromise, loss or damage of sensitive and security classified resources.

PSPF Release 2024 mandates that entities must implement physical security measures to minimise or remove the risk of:

- Requirement 0200: information and physical asset resources being made inoperable or inaccessible, or being accessed, used or removed without appropriate authorisation.
- Requirement 0201: the loss or damage of entity resources, commensurate with the assessed business impact level of their compromise
- Requirement 0202: harm to people.

Categorising physical assets can support entities to identify and consider factors that are relevant to assessing the business impact level of the compromise, loss or damage of the asset—factors that could influence that assessment might include, for example, the desirability of the asset or its level of classification. In turn, this will assist in determining the level and types of protection to apply.

Table 56 describes the categories of assets and provides a number of factors to consider when assessing and determining the business impact level of the compromise, loss or damage of those types of asset.

Table 56: Categories of assets to consider when assessing and determining business impact levels

Asset category	Factors to consider when assessing and determining business impact levels
Type 1A security alarm system	Not applicable
Valuable assets	• The financial viability and lead-time to replace or repair the asset. • The capability of the entity to operate without the asset or with partial functionality of the asset. • The percentage of overall capability to which the asset contributes.
Classified assets	• The level of classification of the asset. • The mobility and accessibility of the classified asset, for example, heavy military equipment.
Important assets	• The integrity of the asset, for example, data with no classification such as human resources data or geographical data for aviation. • The availability of the asset for example a ground transport fleet or firefighting equipment.
Attractive assets	• The desirability of the asset related to its function, for example a physical asset holding information that may be attractive to a foreign adversary. • Portable assets that are desirable, regardless of the information stored on them, for example an iPad.
Significant assets	• The intrinsic value to the national identity.

Asset category	Factors to consider when assessing and determining business impact levels
	• The negative reputational effect of the loss or damage of the asset.
Dangerous assets	• The bulk stores of weapons, such as firearms, explosives and ammunition. • The quantities of hazardous materials that could be weaponised or used to cause harm.

25.1 Authorised Equipment and Commercial Services

The Security Construction and Equipment Committee (SCEC) is responsible for evaluating security equipment for their suitability for use by the Australian Government.

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 and physical assets that do not have a confidentiality BIL of medium or above. ASIO-T4 has developed the Security Equipment Guides to assist entities to select security equipment not tested by SCEC.

Table 57 provides a summary of the equipment that is tested by SCEC and appears in the SEEPL and Security Equipment Guides.

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).

Table 57: SCEC-tested equipment and assigned SL rating

Equipment Type	SL1	SL2	SL3	SL4
Type 1A security alarm system	Not applicable	Not applicable	Not applicable	SCEC
Biometrics devices for access control	SEG 014	SEG 014	SCEC	SCEC
Indoor motion detectors	SEG 002	SEG 002	SCEC	SCEC
Magnetic security switches	SEG 011	SEG 011	SCEC	SCEC
Electronic access control system input devices excluding complete systems	SEG 015	SEG 015	SCEC	SCEC
Key switches – electrical	SEG 008	SEG 008	SEG 008	SEG 008
Electronic key cabinets	SEG 013	SEG 013	SCEC	SCEC
Safes – protection of assets	SEG 022	SEG 022	SEG 022	SEG 022
Stand-alone access control devices	SEG 007	SEG 007	SCEC	SCEC
Mortice locks and strikes	SEG 020	SEG 020	SCEC	SCEC
Magnetic locks	SEG 019	SEG 019	SCEC	SCEC
Electric strikes	SEG 012	SEG 012	SCEC	SCEC

Equipment Type	SL1	SL2	SL3	SL4
Electric mortice locks	SEG 021	SEG 021	SCEC	SCEC
Keying systems	SCEC, SEG 029	SCEC	SCEC	SCEC
Padbolts	SEG 017	SEG 017	SCEC	SCEC
Padlocks chains and hasps	SEG 028 for padlocks Commercial quality	SEG 028 for padlocks Commercial quality	SCEC	SCEC
Hinge bolts	Commercial quality	Commercial quality	SCEC	SCEC
Strike shields and blocker plates	Commercial quality	Commercial quality	Commercial quality	Commercial quality
Cable transfer hinges	Commercial quality	Commercial quality	Commercial quality	Commercial quality
Door closers	SEG 006	SEG 006	SEG 006	SEG 006
Access control portals and turnstiles	SEG 024	SEG 024	SCEC	SCEC
Door operators	SEG 006	SEG 006	SCEC	SCEC
Doors	ASIO Technical Note 1/15 – Physical Security of Zones	ASIO Technical Note 1/15 – Physical Security of Zones	ASIO Technical Note 1/15 – Physical Security of Zones	ASIO Technical Note 1/15 – Physical Security of Zones
Pits	SCEC	SCEC	SCEC	SCEC
Vehicle security barriers	SEG 004 and PSC 166	SEG 004 and PSC 166	SEG 004 and PSC 166	SEG 004 and PSC 166
Perimeter security fences	SEG 003	SEG 003	SEG 003	SEG 003
Window locks	SEG 026	SEG 026	SEG 026	SEG 026
Ballistic treatments	SEG 031	SEG 031	SEG 031	SEG 031
Fragment retention film	SEG 027	SEG 027	SEG 027	SEG 027
Barrier mounted perimeter intrusion detection systems	SCEC	SCEC	SCEC	SCEC
Ground based perimeter intrusion detection systems	SCEC	SCEC	SCEC	SCEC
Volumetric perimeter intrusion detection systems	SCEC	SCEC	SCEC	SCEC
Wafer seals	SCEC	SCEC	SCEC	SCEC and SEG 030
Single use pouches	N/A	SCEC	Not applicable	Not applicable
Shredders	SEG 001	SEG 001	SEG 001	SEG 001
Destructors	SEG 018	SEG 018	SEG 018	SEG 018
Briefcases	SEG 005	SEG 005	SEG 005	SEG 005

25.2 Security Containers, Cabinets and Rooms

Suitably assessed security containers and cabinets are used to secure information, portable and valuable assets and money.

Suitably assessed security containers and cabinets are used to secure information, portable and valuable assets and money. When choosing the most appropriate security container or cabinet, entities should consider:

- the type of asset
- the quantity or size of information and resources
- the location of the information or physical assets within the facility
- the structure and location of the facility
- the access control systems
- other physical protection systems—for example locks and alarm

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 in PSPF Release 2024 details the approach to layering storage containers in security zones.

Recommended Approach

- ✔ Store security classified information and resources security containers and cabinets separately from physical assets to lower the risk of compromise of information if valuable and attractive physical assets are stolen and assist investigators to determine the reason for the incidents involving unauthorised access.

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 valuable, important, attractive, significant or dangerous assets. 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.

For information on SCEC-approved secure containers see the ASIO-T4 Security Equipment Evaluated Products List (SEEPL).

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 can be fire resistant (to protect documents or data), burglar resistant or a combination of the two.

PSPF Release 2024 (Table 41) sets out the minimum commercial safe and vault requirements in the applicable zones based on the business impact level of the compromise, loss or damage to physical assets that are not classified or do not hold any classified information.

For further information on safes and vaults refer to:

- Australian Standard 3809 Safes and strongrooms
- ASIO-T4 Security Equipment Guide SEG-022 Safes—Protection of Assets available to Australian Government security personnel on GovTEAMS.

Recommended Approaches

- Seek advice from qualified locksmiths or manufacturers when deciding the criteria to apply to select commercial safes and vaults.
- Implement other physical controls that give the same level of intrusion resistance and delay where physical assets cannot be secured in commercial safes and vaults. These physical controls may include individual item alarms, alarm circuits or additional out-of-hours guarding.

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 assets and valuable assets, where the compromise, loss or damage would have a business impact level.

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.

25.2.4 Vehicle Safes

Entities may consider fitting vehicles used by field staff with field safes to carry valuable assets and official information. Vehicle safes give some protection against opportunist theft and are only of value when vehicles are fitted with other anti-theft controls.

25.2.5 Managing Security Containers and Cabinets

Security containers and cabinets can be a source of security risk if not managed appropriately over their lifetime. Entities should ensure that keys to security containers and cabinets are secured in key cabinets within a facility's secure perimeter and where possible within the security zone where the containers and cabinets are located.

For security containers and cabinets that are secured using combination settings, entities should ensure that combination settings are changed:

- regularly—not less frequently than every six months
- following repairs
- following change of personnel, and
- when there is reason to believe the setting has been, or may have been compromised.

25.2.6 Key Cabinets

Manual and electronic key cabinets are used to secure keys, for example keys for C Class containers or internal offices, and are normally located within the security zone or in close proximity to the zone where the locks are located. Electronic key cabinets may have automated audit capacity that negates the need to maintain a key register. Electronic key cabinets may also be integrated into the Electronic Access Control System.

The SCEC approved Class B key cabinets provide the same level of protection as SCEC-approved Class B cabinets. SCEC-approved electronic Class C and B key containers are recommended to store keys for security zones four, five and Class C containers.

For advice refer to ASIO SEG-013 Electronic Key Cabinets available for Australian Government security personnel on GovTEAMS.

Commercial grade key cabinets vary in quality and provide very little protection against forced or covert access.

25.2.7 Magazines, Armouries and Explosive Storehouses

Advice on magazines, armouries and explosive storehouses is available from the Department of Defence. Refer to the Defence Security Principles Framework.

25.3 Perimeter Doors, Locks and Hardware for Facilities

Locks can deter or delay unauthorised access to information and physical assets. 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 should:

- secure all access points to their premises, including doors and windows, using commercial-grade or SCEC-approved locks and hardware—these locks may be electronic, combination or keyed
- assign combinations, keys and electronic tokens the same level of protection as the highest classified information or most valuable physical asset contained in the area that is secured by the lock
- use SCEC-approved locks and hardware rated to Security Level 3 in Zones Three to Five (see the Security Equipment Evaluated Product List).
    - entities may use suitable commercial locking systems in other areas

  - entities should assess the level of protection needed from doors and frames when selecting locks, as locks are only as strong as their fittings and hardware
- use SCEC-endorsed locksmiths when using SCEC-approved locks (the SCEC-endorsed locksmith listing can be requested from ASIO-T4 and SCEC), and
- use using doors that provide a similar level of protection to the locks and hardware fitted; refer to Australian Standard AS 3555.1 - Building elements - Testing and rating for intruder resistance - Intruder-resistant panels.

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, and
- levels of protection against compromise techniques, such as picking, impressions and decoding.

When selecting a keying system, entities should evaluate:

- the extent of legal protection offered by the manufacturer
- supplier protection of entity keying data within their facilities
- the transferability of the system and any associated costs, and
- commissioning and ongoing maintenance costs.

Entities should strictly control and limit the number of master keys. The loss of a master key may require re-keying of all locks under that master. Key control measures include regular auditing of key registers to confirm the location of all keys in accordance with the entity's risk assessment.

Recommended Approach

- ✔ Locate key cabinets within a facility's secure perimeter and, where possible, within the perimeter of the Security Zone where the locks are located.

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.

Access control can be achieved in a number of ways, for example:

- security guards located at entry and exit points
- security guards located at central points who monitor and control entry and exit points using intercoms, videophones and closed-circuit television cameras
- mechanical-locking devices operated by keys or codes
- electronic access control systems, or
- psychological or symbolic barriers, can be used for deterrence, but are not considered an effective access control measure, for example signage or crime prevention through environmental design.

Each measure has advantages and disadvantages. The measure or mix of measures selected and used will depend on the particular circumstances in which access control will be applied.

Entities may limit access to technology facilities where the business impact level is lower than catastrophic. Example of mitigation strategies that entities could employ are:

- a dedicated access group in the security alarm system, or electronic access control system (where used), and
- a security guard at the entrance provided with a list of people with a need-to-know or need-to-go into the technology facility.

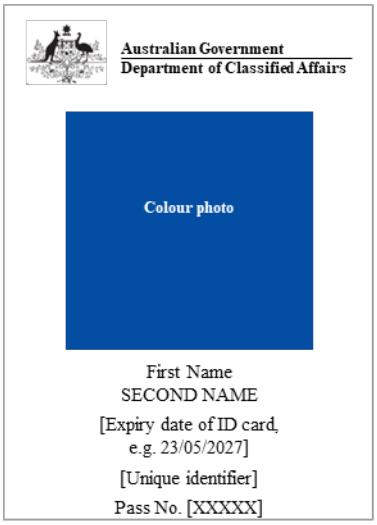
See ASIO Protective Security Circular PSV 149 Physical Security Certification of Outsourced IT facilities for further guidance on the ongoing management of certified outsourced technology facilities. To restrict access to assets within technology facilities, entities should use SCEC-approved tamper-evident wafer seals suitable for application to hard surfaces. These seals give a visual indication of unauthorised access to equipment if the seals are removed or broken. See ASIO-T4 Security Equipment Evaluated Products List available on need-to-know basis on GovTEAMS.

25.4.1 Identity Cards

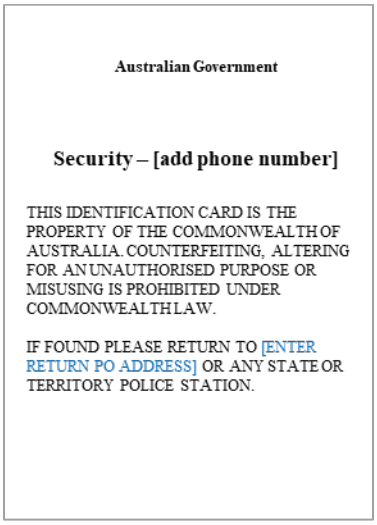
Identity (ID) cards allow the recognition of authorised personnel in entity facilities. Identity cards are an essential access control measure and should:

- only be issued to persons whose identity has been confirmed
- be uniquely identifiable
- be worn by all authorised personnel, authorised contractors and visitors
- be clearly displayed at all times while in entity facilities (and removed outside entity facilities)
- be used in all entity facilities, regardless of the level of the Security Zone
- include a return address for lost cards, and
- be audited regularly in accordance with the entity's risk assessment.

Example of content for identity cards (not mandatory)



FRONT VIEW



BACK VIEW

Identity cards should not:

- be worn outside of entity facilities, or
- identify the facility wo which the card gives access.

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.

See PSPF Guidelines Section 16.1—Pre-Employment Screening for guidance on identity checks and the National Identity Proofing Guidelines.

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).
- 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.

PSPF Requirement 0206 mandates that 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.

Controlling access can include recording visitor details and issuing visitor passes. Visitor registers are used for this purpose and record the visitor name, entity or organisation, purpose of visit, date and time of arrival and departure. Issuing visitor passes for access to Zone Two when other controls to limit access are not in place is also recommended.

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.

Visitors can be issued with electronic access control system cards specifically enabled for the areas they may access. In more advanced electronic access control systems, it is possible to require validation at all electronic access control system access points from the escorting officer.

Entities should escort visitors in Zone Two unless unescorted access is approved. Entities dealing with members of the public are encouraged to use procedures for dealing with unacceptable behaviour on entity premises or unauthorised access to restricted areas.

Regardless of the entry control method used, entities should only allow visitors to have unescorted access if they:

- have a legitimate need for unescorted entry to the area
- have the appropriate security clearance, and
- are able to show a suitable form of identification.

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 assets 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 PSPF Guidelines Section 12.3—International Information Sharing.

25.4.3.2. Event Security

The provision of a safe and secure environment is fundamentally important for the delivery of successful Australian Government events. The Australian Government expects that entities give due consideration to the security of all events they manage, plan or host, whether organised by the entity or outsourced.

Events that need security may include, but are not limited to meetings, conferences, parades, or any gathering where Australian Government people, information or assets are involved. Events may be held at a single or multiple venues, managed by an entity or commercially run venues. Not all events will require additional protective security arrangements but they may be necessary depending on the scale, scope, function, duration or location of the event.

Event security aims to:

- protect personnel, visitors, delegates and guests from violence and intimidation
- protect security classified information and resources from unathorised access, disclosure or compromise
- prevent unauthorised people gaining access that could cause embarrassment to the entity, the government or partners
- protect property from damage
- anticipate any changes in the National Threat Level, or event specific threats, and provide for rapid escalation of security measures, and
- ensure the proceedings are conducted without disruption, and minimising any disruptions to the public.

If the event is to be held overseas, entities should consult with the DFAT in the early planning stages to determine the appropriateness of the proposed location and venue. This is particularly important if the event will involve accessing or using security classified information, or if the event is to be attended by Australian

dignitaries. Entities need to also consider their obligations under Australian legislation and conventions for the protection of foreign dignitaries attending their events.

Before the Event

Australian Government entities have common law duties as well as statutory obligations under Australian and/or state or territory legislation to protect people attending events. Protective security and safety should be considered in the earliest stages of event planning, and protective security arrangements should be identified as part of the event costing.

Event Security Officer

Event organisers should consider whether the event warrants appointment of an Event Security Officer (ESO). The ESO should be competent in security management and risk assessment and be consulted during the planning stages, including venue selection.

Duties of the ESO may include:

- seeking advice on the possible threats to the event
- completing a security risk assessment for the event or venue(s)
- preparing any security plans based on the risk assessment activity
- making necessary security preparations for the event
- coordinating security during the event, and
- liaising with appropriate entity and external authorities before, during and after the event.

Possible Threats

Usually, the consideration of the possible threats to the event and the preliminary work on the plan will occur at the same time. The ESO should seek advice on possible threats from the part of the entity coordinating the event, other relevant areas in the entity and from external entities such as ASIO, the AFP and State or Territory Police.

The ESO should seek a threat assessment from ASIO's National Threat Assessment Centre (NTAC) if:

- the event could be the subject of terrorism or violent protest
- previous similar events have been subject to terrorism or violent protest
- the information to be discussed is classified SECRET or above, and it is considered there may be a risk of compromise, or
- previous experience indicates this is appropriate.

Any request for a threat assessment is to include enough details on the event to enable a robust and thorough assessment of the terrorist or violent protest threats specific to the event.

Entities should inform NTAC if they become aware of any additional relevant information after the original threat assessment is issued. NTAC may also issue updated threat assessments if they become aware of any relevant information.

The National Situation Room (NSR) is a 24/7 crisis management information and whole-of-government coordination facility provided by Emergency Management Australia. The NSR provides whole-of-government all-hazards monitoring and situational awareness for domestic and international events affecting Australia or Australian interests.

Entities may wish to refer to the Australia-New Zealand Counter-Terrorism Committee's Australia's Strategy for Protecting Crowded Places from Terrorism (2023) publication and its supplementary materials on Australian National Security, including the Crowded Places Self-Assessment Tool, for advice on events involving large numbers of attendees, or the public, and where there is a risk of terrorism.

High Office Holders, Diplomats and Foreign Guests

The Australian Government takes seriously its *Vienna Conventions on Diplomatic and Consular Relations* obligations to protect diplomatic missions and consular posts and their staff. These obligations have been adopted into Australian law by the:

- *Diplomatic Privileges and Immunities Act 1967*
- *Consular Privileges and Immunities Act 1972*, and augmented by the
- *Public Order (Protection of Persons and Property) Act 1971*,and
- *Crimes (Internationally Protected Persons) Act 1976*.

Australia also has obligations under the:

- *Convention on the Prevention and Punishment of Crimes Against Internationally Protected Persons, including Diplomatic Agents,* and
- *Foreign States Immunities Act 1985*.

The entity responsible for planning, organising or managing an event should, based on their risk assessment, seek advice where the event is of a non-routine nature and is to be attended by high level officials such as:

- Australian holders of high office—for example Federal Ministers
- high level visiting foreign dignitaries—for example heads of state/heads of government/foreign ministers or other senior level ministers
- members of the diplomatic or consular corps—at ambassador level, or
- controversial visitors who could attract protest activity.

Event organisers should also review the Protocol Guidelines and seek advice from DFAT, Protocol Branch for any events that have high level foreign dignitary attendance.

Event organisations should contact the Department of Home Affairs for major events that the Prime Minister has declared as Special Events.

Event Security Plan

The ESO should develop the security plan based on a risk assessment of the event. As details of the event become clearer, and preparations for the event develop, the plan will evolve and take into account matters including, but not limited to:

- the appropriate level of security for the event
- the duration, location and size of the event
- roles and responsibilities of event staff
- what needs to be protected—for example the proceedings themselves, documents (both those provided and notes taken during the event), people
- whether that need will stay constant throughout the event, or vary from session to session

- the nature of the threats
- who will be involved—for example host personnel only, other entities personnel, non-entity representatives, Australian office holders, office holders of other countries, other VIPs, media representatives, the public
- any security clearance or entity specific character check requirements for attendees
- whether close personal protection of VIPs may be required
- what special protective security measures could be necessary—for example audio counter-measures
- the need for contingency plans; including any communications, command and control arrangements; and alternate venues against particular incidents—for example bomb alerts and public demonstrations
- reception procedures and escort requirements for visitors
- event access and identity passes
- security containers and other security equipment that will be needed
- whether mail will be received or distributed at the event
- who is responsible for AFP or local police liaison, and
- what event security and emergency instructions will be required.

For events that will involve SECRET, TOP SECRET or certain Codeword security classified information the ESO should, based on the risk assessment, seek advice from ASIO-T4 on protection of the information. In such cases the ESO should include in the event security plan what measures can be taken to:

- strictly limit the number of invitees to the overall event
- strictly limit the number of invitees to particular sessions
- limit the duration of the event to as short a period as practicable
- keep handouts to a minimum, and
- secure the meeting room from audio-visual recording devices—seek advice from ASIO-T4 on Technical Surveillance Counter Measures.

Event Venue

There may be a choice of venues, some within the entity's facilities and others at external venues. As far as possible, entities should hold events involving SECRET, TOP SECRET or Codeword information on entity controlled or Australian Government controlled premises. The less control the entity has over the proposed event venue, the more likely additional security measures will be needed.

Venue selection should, based on the event risk assessment, also consider the flow of the event—that is what happens and when and how it all fits together, attendee safety, and transport.

The entity should carry out a preliminary security survey of possible venues at the earliest opportunity. Where possible the ESO should accompany the event organiser during the preliminary inspection. When preliminary security survey is undertaken by the event organiser the ESO should provide advice on security requirements.

If protest activity is a possibility the agency should involve the local police at an early stage of the event planning.

A more detailed inspection might be required later, once a particular venue is selected. At both stages, contact with local police and venue management can be useful to gain local knowledge.

In the site survey entities should consider:

- what is adversely affecting physical security and how easy is it to remedy the problems, including door locks and window catches, curtain fittings, and exterior lights and light fittings
- the ability to maintain control of access to both the venue and to particular rooms, including any on-site parking
- the ability to provide for an area where suspicious articles can be examined (and where detonation of explosive devices would cause minimal damage to property and no injury to people), and
- the vulnerability of the venue to overhearing, overlooking and electronic eavesdropping.

Based on the security plan and survey of the venue, the event organiser may need to address a number of matters before the event, including:

- event set up schedules
- the preparation and issue of any event security instructions—for example:
    - entry control
    - storage and handling of security classified information
    - security classified waste disposal
    - key control procedures
    - emergency evacuation procedures
    - reporting of security incidents, and
    - communication plan.
- arrangements for the supply and delivery of necessary security containers and other security equipment
- the preparation of event access and identity passes
- ensuring that all people present, including visitors and support staff, have the necessary security clearance
- the preparation of any visitor reception procedures and escort requirements for visitors
- the preparation of any key control measures
- the preparation and management of any event security exercises
- arrangements for:
    - conducting technical surveillance counter measures
    - employees or guards to control access, and
    - any necessary searches to sanitise the premises.

25.4.4 Ongoing Third-party Access to Facilites

The Accountable Authority or CS 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.

Entities that face significant threats and those with larger, multi-building facilities may require perimeter access controls to restrict access to their facilities.

25.5.1 Closed Circuit Television

Entities may use closed circuit television as a visual deterrent to unauthorised access, theft or violence and it can assist in post-incident investigations and alarm activation investigations. A closed circuit television system is not a substitute for physical barriers.

To provide appropriate coverage it is important that entities install a sufficient number of cameras to monitor at a minimum:

- the entire perimeter of the tenanted area or building, particularly publicly accessible areas such as the reception lobby or entry points
- all facility access points, including car park entrances
- public access hallways, stairwell and lift lobbies
- inside loading docks, and
- public area boundaries; that is, where there is delineation between a public and security zone.

Where closed circuit television images have been used in an incident investigation, entities should ensure these images are stored in a secure storage container, selected to maintain evidentiary integrity, for a minimum of 31 days post-incident investigation.

Recommended Approach

- Seek specialist advice in the design of closed circuit television management systems.

25.5.2 Security Lighting

Internal and external lighting is an important contributor to physical security. It can be used as a deterrent, to detect intruders, to illuminate areas to meet requirements for closed circuit television coverage, assist response teams when responding to incidents at night and to provide personnel with safety lighting in car parks and building entrances. Entities may use motion-detection devices to detect movement and activate lighting as an additional deterrent.

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.

PSPF Requirement 0208 mandates that unauthorised access to Security Zones One to Five is controlled in accordance with the physical security measures and controls for security alarm systems.

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.

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, and
- Class 5 is suitable for protection of information and physical assets 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 assets 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 assets 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.

- 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.

25.8 Security Guards

Security guards provide deterrence against loss of information and physical assets 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.

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.

Security guards provide deterrence against loss of information and physical assets 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.

Recommended Approach

- Response time for off-site guards should be less than the delay given by the total of other controls.
- Guarding response time to alarms to should be within the delay period given by the physical security controls, although, the highest level of assurance is provided by on-site guards who can respond immediately, 24 hours, seven days a week.
- Determine the requirement for guards (their duties and the need for and frequency of patrols) on the level of threat and risk.
- Assess the security clearance requirement for guards based on the security zone requirements and frequency of access.

- Only employ, either through the entity or through a commercial guarding company, guards who are licensed in the jurisdiction where they are employed.

25.8.1.1. Out-of-Hours Guarding

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 ISM for controls to protect technology used for security classified discussions.

25.10 Physical Security Measures and Controls Mandatory Elements

PSPF Release 2024 (Tables 42–48) detail the mandatory physical security measures and control elements for each Security Zone. See PSPF Guidelines Sections 25.2 – 25.8 for guidance on these mandatory elements.

25.10.1 Physical Resources

Physical resources are tangible assets that are valuable to an entity and require protection. This protection includes ensuring their continued operability and accessibility, as appropriate, and preventing any unauthorised access, use or removal.

Physical resources can be categorised as follows:

- valuable – the asset's monetary value
- classified – the asset is classified in its own right or is classified due to the confidentiality requirements of the information held on the asset, for example IT equipment
- important – the significance of the asset's integrity or availability for the entity's operations
- attractive – the asset is not necessarily valuable but is desired, for example an iPad
- significant – the asset has cultural or national significance, regardless of monetary value, and
- dangerous – the asset's likelihood to inflict harm, for example weapons or chemical, biological, radiological and nuclear hazards.

The protections required for, and that can effectively be applied to, different physical resources will be affected by the category of asset and the business impact level of the compromise, loss or damage of the resource, as described below.

25.10.2 Asset Control for Physical Resources

Asset control involves identifying holdings of resources and establishing accountability mechanisms that protects them against theft, damage and loss. Asset control procedures may include:

- recording the location and authorised custodian of resources
- periodic auditing of resources, and
- reporting requirements for the loss or damage of resources.

Entities should determine the business impact level as part of the security risk assessment process for managing the risks associated with protecting entity resources. PSPF Release 2024 (Table 3) details the business impact levels relating to compromise of the confidentiality of information.

Recommended Approach

- Entities may, as a result of their risk assessment, consider that more frequent audits are appropriate for higher risk resources, for example valuable assets, attractive assets and assets of cultural significance.

26 Glossary

26.1 Glossary of Abbreviations

Abbreviation	Meaning
ACSC	Australian Cyber Security Centre
AFP	Australian Federal Police
AGAO	Australian Government Access Only
AGCMF	Australian Government Crisis Management Framework
AGRkMS	Australian Government Recordkeeping Metadata Standard
AGSCS	Australian Government Security Caveat Standard
AGSVA	Australian Government Security Authorised Vetting Agency
APS	Australian Public Service
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
ASIS	Australian Secret Intelligence Service
AUPDNS	Australian Protective Domain Name Service
AUSTEO	Australian Eyes Only
AVA	Authorised Vetting Agency
BCA	Building Code of Australia
CDR	Classified Document Register
CISO	Chief Information Security Officer
COMSO	Communications Intelligence Security Officer
CSO	Chief Security Officer
DFAT	Department of Foreign Affairs and Trade
DOS	Department of State
DTA	Digital Transformation Agency
DVS	Document Verification Service
EACS	Electronic Assess Control Systems
Entity	Non-Corporate Commonwealth Entity
EPMS	Email Protective Marking Standard
FOCI	Foreign Ownership, Control or Influence
GSA	General Security Agreements
GSC	Government Security Committee
HCF	Hosting Certification Framework
ICT	Information Communications Technology
IED	Improvised Explosive Devices
IMM	Information Management Markers
IRAP	Infosec Registered Assessors Program
ISM	Information Security Manual

Abbreviation	Meaning
ISO	International Organization for Standardization
IT	Information Technology
LES	Locally Engaged Staff
MOP(S)	Members of Parliament (Staff) Act 1984
MOU	Memorandum of Understanding
NAP	Normal Administrative Practice
NSC	National Cyber Security Committee
NSR	National Situation Room
NV1	Negative Vetting 1
NV2	Negative Vetting 2
ONI	Office of National Intelligence
OT	Operational technology
PDNS	Protective Domain Name System
PIDS	Perimeter Intrusion Detection Systems
PMC	Department of the Prime Minister and Cabinet
PSB	Protective Security Board
PSC	Protective Security Circular
PSPF	Protective Security Policy Framework
PV	Positive Vetting
SAS	Security Alarm System
SCEC	Security Construction and Equipment Committee
SCI	Sensitive Compartmented Information
SCIF	Sensitive Compartmented Information Facilities
SCSA	Security Clearance Suitability Assessment
SEEPL	SCEC Security Equipment Evaluated Product List
SEG	Security Equipment Guide
SL	Security Level
SSPE	Shared Service Provider Entity
TSCM	Technical Surveillance Countermeasures
TS-PA	TOP SECRET-Privileged Access
VDP	Vulnerability Disclosure Program
PEN	Policy Explanatory Note
PGPA	Public Governance, Performance and Accountability Act 2013 (Cth)
BIL	Business Impact Level
FVEY	Five Eyes

26.2 Glossary of Terms

Term	Meaning
Accountable Authority	The person or people responsible for, and with control over, a Commonwealth entity's operations. This is set out in Section 12 of the Public Governance, Performance and Accountability Act 2013 (Cth).
Accountable Material	Information that requires the strictest control over its access and movement, including TOP SECRET information, all codeword information, select special handling instruction caveats and any classified information designated as accountable material by the originator.
Aggregated Information	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.
Alternative Mitigation	Control or standard that differs from the PSPF Requirement or standard but achieves the same intent and level of protection as the PSPF requirement.
ASIO Outreach	ASIO's public facing outreach area. They provide advice to government, industry and academia on current and emerging security threats, and security policy.
ASIO Technical Notes	Describe the minimum physical security requirements for the construction of Australian Government Security Zones One to Five and SCIFs where security classified information, resources and/or classified equipment is stored, handled, processed or discussed.
Assessing Officer	Person who is appropriately qualified and competent to conduct personnel security clearance assessments in accordance with the procedures outlined in the PSPF.
Authorised Vetting Agency	An Australian Government entity that is authorised to undertake security and grant security clearances. Authorised Vetting Agencies include AGSVA, ASIO, ASIS, ONA, AFP and DFAT.
Authorising Officer	Person authorised to make informed risk-based decisions on the security risks associated with the operation of a technology system and grant authorization for the system to operate.
Baseline Security Clearance	Clearance level required for ongoing access to security classified information at the PROTECTED level, or where a level of assurance is required of a person's suitability to perform a role.
Chief Information Security Officer	An officer with appropriate capability and a minimum security clearance of Negative Vetting Level 1, who is responsible for cyber security leadership in the entity and ensuring compliance with cyber security requirements, policy, standards, regulations and legislation.
Chief Security Officer	A senior executive officer (or EL2 officer if the entity has fewer than 100 people), with appropriate seniority and a minimum security clearance of Negative Vetting Level 1, who is responsible for oversight of entity protective security arrangements.
Classified Document Register	Record of TOP SECRET information and accountable material detailing copies received, location, transfer and disposal.
Clear Desk Policy	Policy requiring entity personnel to securely and appropriately store security classified information and valuable resources when absent from the workplace.
Codewords	Sensitive compartment information that requires a compartmental briefing.
Compartmental Briefing	Mechanism for restricting access to security caveated (Codeword) information to individuals who have been 'briefed' and trained on the particular requirements and sensitivities that apply to the caveat by the relevant authority.
Controlling Authority	The entity/s that originated the information marked with the security caveat, established the additional special protections and handling requirements and is responsible for managing and administering the security caveat.
Cyber Security	Measures used to protect the confidentiality, integrity and availability of information technology (IT) and operational technology (OT) systems, applications and data.
Declassification	Administrative decision by the originator to reduce the security classification of information to OFFICIAL (an unclassified state) when it no longer requires security classification handling protections.

Term	Meaning
Delegate	Responsibilities and powers can only be delegated where explicitly stated in the PSPF.
Dual National	Person who holds citizenship of two or more countries.
Eligibility Waiver	An Accountable Authority's decision to waive the citizenship or checkable background eligibility requirement for a candidate to hold a security clearance where there is an exceptional business requirement and after conducting a risk assessment.
Employment Screening	Checks to confirm the background and identity of potential employees or engagement of contractors.
Encryption	Process of transforming data into an unintelligible form to enable secure transmission.
Entity	Any Commonwealth entity listed under paragraph 10(1) of the PGPA Act. For the purposes of the PSPF Requirements, entity refers to non-corporate Commonwealth entity.
Entity Facilities - Domestic	Physical premises or space that the entity occupies in Australia to perform its approved functions. Facilities can be a building, floor of a building or designated space.
Entity Facilities - International	Physical premises or space that the entity occupies outside of Australia to perform its approved functions. Facilities can be a building, floor of a building or designated space.
Exceptional Circumstances	Situations beyond the entity's control that are not routine in nature, not enduring, and are unforeseen, unavoidable or unexpected.
Five Eyes	Anglosphere intelligence alliance comprising Australia, Canada, New Zealand, the United Kingdom, and the United States.
Foreign Entity	A person, business or organisation that is related to, or comes from, a country other than Australia.
Foreign Interference	Activity carried out by, or on behalf of, or in collaboration with, a foreign power that is clandestine or deceptive and is carried on for intelligence purposes; is carried on for the purposes of affecting political or governmental processes; or is otherwise detrimental to the interests of Australia; or involves a threat to any person.
Foreign National	A person who is not an Australian citizen.
Foreign Ownership, Control or Influence (FOCI)	An organisation is considered to be operating under FOCI when a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, through the ownership of the company under the purview of its National Security Authority/Designated Security Authority, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that entity 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.
Foreign Power	Foreign governments or entities under their direction or control, or foreign political organisations working to undermine Australia's national security or advantage a foreign power.
Gateway	Gateways securely manage data flows between connected networks from different security domains.
GovTEAMS	Collaboration service for the Australian Public Service. The OFFICIAL: Sensitive components of the PSPF are published on the Department of Home Affairs' Protective Security Policy GovTEAMS community. Only government personnel with a government email address may access this community.
Hardware	A generic term for IT equipment and OT equipment
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.
Information Compromise	Includes, but is not limited to information loss, misuse, interference, unauthorised access, unauthorised modification, or unauthorised disclosure.
Information Management Markers	Optional way for entities to identify information that is subject to non-security related restrictions on access and use.

Term	Meaning
Infosec Registered Assessors Program (IRAP)	An initiative of ASD designed to register suitably qualified individuals to carry out security assessments for systems.
Insider	Any person that has, or had, authorised logical or physical access to a system and its resources.
Insider Threat	An insider that performs, or attempts to perform, damaging activities (either intentionally or unintentionally) to a system or its resources. Some organisations may choose to exclude unintentional damage to systems and their resources (often referred to as negligent or accidental damage) from their definition of insider threat in order to focus on insiders with malicious intent (often referred to as malicious insiders).
Integrated Information	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.
Integrity	In the security context, integrity is defined as a range of character traits that a clearance subject possesses (and demonstrates) in order for the government to have confidence in their ability to protect Australian Government resources.
Lockable Cabinet	Cabinet that is commercially available, of robust construction and is fitted with a commercial lock.
Loyalty	Commitment to Australia and the democratic processes of the Australian Government. Loyalty is not confined to the nation but also includes the objectives, ethos and values of the working environment (strong political views incompatible with the Australian democratic system of government may put a person's loyalty in doubt).
Mobile Device	A portable computing or communications device, including smart phones, handheld computers, tablets, laptops and digital assistants that use a mobile operating system.
Mobile Device (Government-Issued)	Mobile or portable computing communications device that is owned and issued by an Australia Government entity to access government systems and information, configured, encrypted and managed to ASD standards and guidance and is approved by the relevant authority to process, store or communicate entity information of a specified classification. This includes Australian Government-issued mobile devices that for operational reasons are connected to isolated networks, for example standalone or air gapped devices.
Mobile Device (Authorised Non-Government)	Mobile or portable computing communications devices owned or issued by a non-government source (for example commercial organisation, non-government organisation, industry-issued or privately owned) that is configured, encrypted and managed in accordance with ASD standards and guidance, and the residual risk is accepted by the Australian Government entity system risk owner to access, process, store or communicate OFFICIAL, OFFICIAL: Sensitive, PROTECTED Australian Government information or data.
Mobile Device (Other Non-Government)	Devices that are not owned, issued or authorised by the entity. 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. 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.
National Interest	Maintenance of Australia's good international reputation and bilateral relations, public confidence in the areas of tourism, trade, the economy and government, and the security and safety of all Australians.
Need-to-Know	Principle of restricting an individual's access to only the information they require to fulfil the duties of their role.

Term	Meaning
National Security Authority	Entity responsible for general oversight of General Security Agreements and other international arrangements where Australian Government security 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 is the National Security Authority for the Australian Government.
Negative Vetting	An evaluation process used when obtaining certain security clearances that relies on the absence of information to the contrary in order to assess the subject's suitability for that security clearance.
Organisational Suitability Assessment	Series of checks, based on an entity's enterprise risk tolerance, to determine an individual's suitability to work for that entity.
Originator	The entity responsible for creating and classifying an official record where a record is as defined in the *Archives Act 1983* (Cth). The entity remains the sole and permanent owner of the classification.
Password	A sequence of characters used for authentication.
Patch	A piece of software designed to remedy vulnerabilities or improve the usability or performance of software, IT equipment or OT equipment.
Personnel	Employees and contractors, including secondees and any service providers that an entity engages. It also includes anyone who is given access to Australian government resources held by the entity as part of entity sharing initiatives.
Personal Security File	Electronic or paper file containing sensitive personal information and other information used to make a decision on a person's suitability to hold and maintain a security clearance. Includes a record of the checks, decisions, risk assessments, mitigations, conditions and all other information relating to a security clearance.
Policy Explanatory Note	Provide advice and further information on specific security issues or topics that are not explicitly addressed in the PSPF, but there is an expectation that entities are managing the risks of.
Portfolio Entity	A government body that falls within a minister's area of responsibility, or portfolio, in the Australian Government. For example, The Treasury portfolio includes the Australian Bureau of Statistics, the Australian Competition and Consumer Commission, and the Australian Office of Financial Management.
Positive Vetting	A system of security checking that attempts to examine and independently verify all relevant aspects of a subject's suitability to hold certain security clearances. Positive vetting requires more extensive checks than negative vetting. TS-PA security clearance is replacing Positive Vetting.
Principles	Fundamental values that guide decision–making. There are 6 principles that inform protective security setting.
Procedural Fairness	Principles that require that individuals whose rights, interests or expectations are adversely affected, be informed of the case against them and be given an opportunity to be heard by an unbiased decision-maker and respond. Procedural fairness gives regard to ensuring the security integrity of any current or future investigation of the entity or of another entity.
Protective Security	The protection of information, people and physical assets.
Reclassification	Administrative decision by the originator to change the security classification of information based on a reassessment of the potential impacts of its compromise. Reclassification may raise or lower the security classification of information.
Requirement	Mandatory obligation that non-corporate Commonwealth entities must implement to achieve minimum protective security standards.
Resources	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.

Term	Meaning
Review for Cause	Process where the Authorised Vetting Agency reviews a clearance holder's eligibility and suitability to hold a security clearance where concerns are identified. 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.
Risk Appetite	The risk an entity is willing to accept or retain within its tolerance levels to achieve its objectives, as defined in the Department of Finance Risk Management Policy.
Risk Tolerance	The levels of risk an entity will tolerate to achieve a specific objective or manage a category of risk, as defined in the Department of Finance Risk Management Policy
Safe Hand	Method of dispatching security classified information or resources to the addressee in the care of an authorised person or succession of authorised people who are responsible for its carriage and safekeeping.
Sanitisation	Process to remove, conceal or change information by editing, redacting or altering information to reduce its security classification to protect intelligence, sources, methods, capabilities, analytical procedures or privileged information.
Secondee	A person on exchange, loan or long-term posting to an entity, who retains employment with their original employer.
Secure by Design	A software development principle whereby security is designed into every stage of a product or service's development.
Security Practitioner	Personnel appointed to perform security functions or specialist services related to security within an entity. These personnel support the work of the Chief Security Officer and Chief Information Security Officer.
Security Assessment	An activity undertaken to assess controls for a system and its environment to determine if they have been implemented correctly and are operating as intended.
Security Assessor	Person authorised to review the system architecture and documentation, and assesses the implementation and effectiveness of security controls. These assessments are typically undertaken by an IRAP assessor or entity personnel with the appropriate capability.
Security Caveat	A marking that indicates that the information has special handling requirements in addition to those indicated by its security classification. There are four categories of caveats: Codewords, Foreign Government Markings, Special Handling Instructions and Releasability Caveats.
Security Classification	The Australian Government uses 4 security classifications: OFFICIAL: Sensitive, PROTECTED, SECRET and TOP SECRET. All other information from business operations and services is OFFICIAL.
Security Clearance Delegate	A person formally authorised to make decisions on the outcome of a vetting process—to grant, deny, grant-conditional, revoke or cancel a security clearance.
Security Clearance Process	Process of assessing a person's suitability to have access to Australian Government security classified information.
Security Construction and Equipment Committee	An Australian Government interdepartmental committee responsible for the evaluation and endorsement of security equipment and services. The committee is chaired by the Australian Security Intelligence Organisation.
Security Culture	The characteristics, attitudes and habits within an entity that establish and maintain security.
Security Governance Committee	A senior committee that supports the Accountable Authority and CSO to achieve protective security objectives and monitor performance against those objectives. Especially valuable to entities with large or complex arrangements.
Security Plan	Central document detailing how the entity plans to manage and address their security risks.
Security Risk	The effect of uncertainty on objectives that is often measured in terms of its likelihood and consequences. Something that could result in compromise, loss, unavailability or damage to information or physical resources, or cause harm to people.
Security Risk Management	The process of identifying, assessing and taking steps to reduce security risks to an acceptable level.
Security Vetting	The evaluation of a person's suitability to obtain and maintain a security clearance and access sensitive and classified Australian Government resources.

Term	Meaning
Security Zone	Restricted access areas with increasing restrictions and access controls as the Security Zones progress from Zone One to Zone Five, primarily to protect the security classified information, resources or activities that will be processed, stored or communicated in that area.
Security-in-Depth	Multi-layered system in which security measures combine to make it difficult for an intruder or authorised personnel to gain unauthorised access to technology assets and their components.
Service Provider	Person or company that provides a product or service to the entity or its operations.
Shared Security Risk	Security risks that extend beyond a single entity and which require a collaborative effort of shared oversight and management and may involve external stakeholders, other sectors and jurisdictions. In large, complex entities, shared risk can exist within the entity as well as between them.
Sponsoring Entity	The Australian Government entity that sponsors an individual's security clearance.
Standard	PSPF Standards detail additional mandatory requirements and policy on specific protective security topics, and are more granular and prescriptive in nature.
System	Related set of hardware, software and supporting infrastructure used for the processing, storage or communication of information/data and the governance framework in which it operates.
System Owner	Person responsible for ensuring the secure operation of the technology system.
Technical Manual	Technical Manuals are standard or technical controls authorised by the PSPF and maintained by the relevant Technical Authority Entity.
Technology System	Collective term for information technology and operational technology systems.
Third Party	Any partner, consultant, vendor, service provider or supplier that provides a product or service to your entity or its operations.
Unacceptable Level of Risk	When the identified security risks cannot be mitigated to a reasonable or acceptable level, or the security risks to 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.
Vetting Analyst	Person within or authorised by an Authorised Vetting Agency to conduct vetting assessments and assesses a clearance subject and identify any vulnerabilities that may compromise Australian Government resources.
Vetting Delegate	Person formally authorised to make decisions on the outcome of a vetting process (i.e. grant, deny, grant-conditional, revoke or cancel an Australian Government security clearance).
Vetting Personnel	All those involved in conducting the security clearance vetting process, including administrative staff, checking officers, vetting analysts, vetting practitioners, assessing officers, vetting managers and vetting delegates.
Visitors	Person who is not authorised to have ongoing access to all or part of an entity's facilities.