Glossary

A Glossary of common and complex terms used in the Protective Security Policy Framework (PSPF) and their definitions.

Term	Meaning
Accountable authority	The accountable authority of a Commonwealth entity is the person or group of persons responsible for, and with control over, the entity's operations. This is set out in Section 12 of the *Public Governance, Performance and Accountability Act 2013* (Cth).
Alternative mitigation	Alternative security measures or controls that provide at least the same level of protection as the PSPF requirement and may exceed the required level of protection.
Authorised vetting agency	An Australian Government entity that is authorised to undertake security vetting and issue personnel security clearances.
	The Australian Government Security Vetting Agency (AGSVA) is the central vetting agency for the Australian Government. AGSVA can issue security clearances that are sponsored by any Australian Government entity
	There are six (6) non-corporate Commonwealth entities that are authorised to issue security clearances for their own personnel:
	(AFP) (ASIO) (ASIS) (ONI) (DFAT) is authorised to issue security clearances at the Baseline, Negative Vetting 1 and Negative 2 levels (ASIC) is authorised to issue security clearances at the Baseline level only.
Caveat owner	The entity that creates official records with special handling requirements that are in addition to the security classification. For more information see the *Sensitive Material Security Management Protocol (SMSMP).*
Chief Security Officer (CSO)	The Senior Executive Service (SES) level officer appointed by the accountable authority to be responsible for oversight of entity security arrangements across governance, information, personnel and physical security. Provisions for appointing a CSO in an entity with fewer than 100 employees are outlined in PSPF policy: Role of accountable authority.
Core requirement	The requirements that entities must meet to achieve the government's desired protective security outcomes. There are 16 policies which each include a core requirement (as well as supporting requirements).
Eligibility waiver	An accountable authority's decision to waive the citizenship or checkable background eligibility requirement of a candidate to hold a security clearance where there is an exceptional business requirement and after conducting a risk assessment.
Entity	Any Commonwealth entity listed under paragraph 10(1) of the *Public Governance, Performance and Accountability Act 2013 (Cth)*
Lead protective security entity	A Commonwealth entity with additional responsibilities as:

Term	Meaning
	a) lead entity in their portfolio b) provider of government protective security advice, policy, technical standards or intelligence services or c) provider of shared services arrangements.
Negative vetting	As part of the process for obtaining certain security clearances, this is an evaluation process that relies on the absence of information to the contrary in order to assess the subject's suitability for that security clearance.
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.
Outcomes	The protective security aims of the government relating to governance, people, information and physical assets. The PSPF has four security outcomes for entities to achieve as part of the PSPF implementation.
Personal security file	A record of the checks undertaken, decisions undertaken, risk assessments, mitigations, conditions imposed and all other information relevant to a security clearance.
Personnel	Employees and contractors, including secondees and service providers engaged by the entity as well as anyone who is given access to Australian government resources held by the entity as part of entity sharing initiatives
Positive vetting	As part of the process for obtaining certain security clearances, this is a system of security checking that attempts to examine and independently verify all relevant aspects of a subject's suitability for a security clearance—positive vetting requires more extensive checks than negative vetting.
Protective security	The protection of information, people and physical assets.
Principles	Fundamental values that guide decision-making. There are five principles that inform protective security settings (refer to Securing government business: Protective security guidance for executives).
PSPF maturity rating	The level to which an entity has addressed and implemented the core and supporting requirements as outlined in the PSPF. There are four levels of PSPF maturity.
Risk appetite	The risk an entity is willing to accept or retain within its tolerance levels in order to achieve its objectives, as defined in the *Department of Finance Risk Management Policy.*
Risk tolerance	An entity's tolerated levels of risk taking to achieve a specific objective or manage a category of risk, as defined in the *Department of Finance Risk Management Policy*.
Security advisors	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.
Security caveat	Indications of special handling requirements additional to those indicated by security classification. See *Australian Government Security Caveat Guidelines* for more detail.

Term	Meaning
Security culture	The characteristics, attitudes and habits within an organisation that establish and maintain security. Security culture is critical to supporting an entity to appropriately manage security risks.
Security Governance Committee	A senior committee that supports an accountable authority and CSO in achieving protective security objectives and monitoring 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. For further detail see PSPF policy 3: Security planning and risk management.
Security maturity	The entity's capability to holistically and appropriately manage their security risks through effectively implementing and managing the PSPF core and supporting requirements in the context of the entity's specific risk environment and risk tolerances.
Security risk	Something that could result in compromise, loss, unavailability or damage to information or physical assets, or cause harm to people.
Security risk management	Managing risks related to an entity's information, people and physical assets.
Security incident	A security incident is defined as an: a) **action**, whether deliberate, reckless, negligent or accidental that fails to meet protective security requirements or entity-specific protective security practices and procedures that results, or may result in, the loss, damage, corruption or disclosure of official information or resources (see PSPF policy 2: Management structures and responsibilities C.7.1 Security incidents) b) **approach** from anybody seeking unauthorised access to official resources c) observable **occurrence or event** (including natural disaster events, terrorist attacks etc) that can harm Australian Government people, information or assets. For further detail, see PSPF policy 2: Management structures and responsibilities. This also provides details about reporting channels for particular security incidents.
Security vetting	An assessment by an authorised vetting agency of a clearance subject's suitability to hold a security clearance.
Sponsoring entity	The Australian Government entity that sponsors an individual's security clearance.
Supporting requirement	The necessary actions to implement core requirements and attain the government's desired protective security outcomes. There are 16 policies which each include supporting requirements to support implementation of the policy's core requirement.
T4 Protective Security (T4 or ASIO T4)	ASIO's protective security capability (T4) provides expert protective security advice and training to the Australian Government, state and territory governments, and business. This includes physical security certification advice (as defined in the PSPF), technical surveillance

Term	Meaning
	countermeasures, and resources for security managers to assist in the protection of their information, people and assets via the ASIO Business and Government Liaison website. T4 evaluates protective security products (such as locks, alarms and detection devices) to determine their suitability for use in government facilities. T4 provides protective security advice for Australian Government agencies. With the written approval of the Attorney-General, T4 can provide such services to, state and territory governments, business enterprises and critical infrastructure owners, provided that a Commonwealth interest can be shown.
Vetting	The evaluation of a person's suitability to obtain and maintain a security clearance and access sensitive and classified Australian Government resources.
Vetting entity	An authorised entity responsible for assessing a person's suitability to obtain and maintain a security clearance.
Vetting personnel	Vetting officers and delegates who assess a clearance subject and identify any vulnerabilities that may compromise Australian Government resources.

Acronyms

Acronym	Meaning
ACSC	Australian Cyber Security Centre
AFP	Australian Federal Police
AGSVA	Australian Government Security Vetting Agency
APS	Australian Public Service
APSC	Australian Public Service Commission
ASD	Australian Signals Directorate
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security and Intelligence Organisation
ASIS	Australian Secret Intelligence Service
CSO	Chief Security Officer
DFAT	Department of Foreign Affairs and Trade
EACS	Electronic Access Control Systems
ISM	Information Security Manual
IRAP	Information Security Registered Assessor
OAIC	Office of the Australian Information Commissioner
ONI	Office of National Intelligence
PGPA Act	*Public Governance, Performance and Accountability Act 2013* (Cth)

Acronym	Meaning
PSPF	Protective Security Policy Framework
SCEC	Security Construction and Equipment Committee
SES	Senior Executive Service
SMSMP	Sensitive Material Security Management Protocol
TSCMs	Technical Surveillance Countermeasures