Australian Government
Fair Work Building & Construction

Australian Government
Fair Work OMBUDSMAN

Designated Security Assessed Positions & Positions of Trust Guidelines

CHANGE HISTORY

Update the following table as necessary when this document is changed:

Name	Date	Nature of Change
Craig Smith	17 Apr 2012	Draft submission
Craig Smith	10 May 2012	Final submission to ACP Board
Craig Smith	17 May 2012	ACP Board approval
Craig Smith	23 May 2012	Deletion of SES acting for 6 months or more
Craig Smith	20 June 2012	Change of ABCC crest to FWBC and reference to the ABCC in the document.

Table of Contents

1. *Overview*

Except where otherwise specified, these guidelines apply equally to the Fair Work Ombudsman (FWO) and the Fair Work Building & Construction (FWBC), known from this point forward as the 'Agency'.

2. *Agency Head Statement*

*To comply with the Australian Government Protective Security Policy Framework (PSPF) all agencies **MUST** as part of their risk management approach to protective security, identify Designated Security Assessed Positions (DSAPs) and Positions of Trust (PoT) within their organisations.*

As a joint collaborative approach, the agency heads strongly support the direction to employ a risk management approach to personnel security as consistent with the protective security principles.

3. *Protective Security Policy Framework*

2.1 PSPF Core Personnel Security Policy

The core policies of the PSPF provide the mandatory requirements for protective security in Australian Government agencies. The protection of classified resources across Government includes limiting access to those people whom the Australian Government assesses to be suitable and whose work responsibilities specifically require them to access these resources.

2.2 PSPF Personnel Security Mandatory Requirements

The purpose of personnel security is to provide a level of assurance as to the honesty, trustworthiness, maturity, tolerance and loyalty of individuals who access Government resources.

The Agency is adherent to the PSPF mandatory requirements, which state:

- **PERSEC 1 –** All agencies **MUST** ensure that Australian Government employees, contractors and temporary staff who require ongoing access to Australian Government information and resources:
    - are eligible to have access
    - have had their identity established
    - are suitable to have access, and
    - are willing to comply with the Government's policies, standards, protocols and guidelines that safeguard that agency's resources (people, information and assets) from harm.

  Access to higher levels of classified resources is dependent upon the granting of the requisite security clearance.

- **PERSEC 2 -** All agencies **MUST**, as part of their risk management approach to protective security, identify Designated Security Assessment Positions (DSAPs) within their organisation that require acces to CONFIDENTIAL, SECRET and TOP SECRET assets and information. Agencies **MUST** ensure that security vetting is only applied where it is necessary.
- **PERSEC 3** – Agencies **MUST** maintain a DSAP register.

- **PERSEC 4** – Security clearances **MUST** be sponsored by an Australian Government agency. Security clearances are not available on demand or on a speculative basis.
- **PERSEC 5** – All Australian Government agencies **MUST** follow the Australian Government Personnel Security Protocol for personnel security as contained in supplementary material within the PSPF. Only the AGSVA and exempt agencies can grant, continue, deny, revoke or vary a security clearance.
- **PERSEC 6** – Agencies **MUST** have in place personnel security aftercare arrangements, including the requirement for individuals holding security clearances to advise the AGSVA of any significant change in personal circumstance that may impact on their continuing suitability to access security classified resources.

4. *Agency Security Clearance Requirements*

3.1 Need-to-Know Principle

In adherence to the need-to-know principle, the Agency is to limit the access to and dissemination of security classified information or resources to employees who need to use or access the information or resources to do their work and, for ongoing access hold the appropriate level of clearance.

3.2 Security Clearance

A security clearance is an administrative determination by the Agency Security Adviser or Security delegate that an individual is eligible and suitable, from a security stand-point, to access security classified resources. The responsibility for deciding whether to grant, deny, vary or revoke a clearance lies with the Australian Government Security Vetting Agency (AGSVA), or an exempt agency. An agency head has the authority to impose conditions of employment on APS employees that may include “security and character clearances” (section 22(6)(d) of the PS Act).

3.3 Security Clearance Levels

There are four security clearance levels:

- **Baseline Vetting** – ongoing access to information or resources classified PROTECTED, or other situations where an agency might determine it needs a high level of assurance of a person’s suitability to perform a particular role.

- **Designated Security Assessment Positions**
  - **Negative Vetting Level 1** – ongoing access to information or resource classified PROTECTED, CONFIDENTIAL and SECRET, or other situations where an agency might determine it needs a higher level of assurance of a person’s suitability to perform a particular role.

  - **Negative Vetting Level 2** – ongoing access to information or resources classified PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET, or other situations where an agency might determine it needs the highest level of assurance of a person’s suitability to perform a particular role, and

  - **Positive Vetting** – permits access to information or resources at all classification levels including certain types of caveated, compartmented and codeword information. Positive vetting requirements are managed by the Inter-Agency Security Forum on behalf of the Australian Intelligence Community.

The following table summarises the access permitted by each clearance level:

		TOP SECRET	SECRET	CONFIDENTIAL	PROTECTED (and Cabinet information)	DISSEMINATION LIMITING MARKER	UNCLASSIFIED
CLEARANCE	**Negative vetting level 2**	Yes	Yes	Yes	Yes	Yes	Yes
	Negative vetting level 1	**NO**	Yes	Yes	Yes	Yes	Yes
	Baseline vetting	**NO**	**NO**	**NO**	Yes	Yes	Yes
Pre-engagement staff screening		**NO**	**NO**	**NO**	Limited access if screened to AS:4811-2006*	Agency discretion	Yes

* Limited access is access under supervision to information or resources needed to perform the person's duties for periods not exceeding three months.

3.4 Determination of a Security Clearance

Employees of the Agency who are responsible for the ongoing creation, use, handling, storage and disposal of security classified information and resources are to hold a security clearance at the appropriate level of access.

Requesting a security clearance will be in the form of a notification email to the Agency Security Adviser with a business case for the clearance and evidential approval from the requestees immediate Manager.

The Agency Security Adviser will examine all cases for additional needs based on operational requirements and in accordance with the PSPF guidelines, higher level of clearances such as Records Management and Information Technology.

3.5 Clearance Holders Responsibility

Personnel who hold a security clearance are granted the clearance by AGSVA, after careful consideration of all relevant information, including personal circumstances, on a whole of life assessment. Where there is a change in circumstances the decision to grant a clearance may need to be reconsidered.

Agency security clearance holders are to report any changes in their circumstances (reportable circumstances) at the time of the change to AGSVA by submitting a Change of Circumstances Notification Form and provide an information copy to the Agency Security Adviser.

Managers should report any changes in circumstances relating to their staff if they become aware of these changes and are unsure whether the changes have been notified by the clearance holder to the Agency Security Adviser.

All Agency employees should report significant changes in circumstances in other individuals where they feel it may impact on Agency security to the Agency Security Adviser.

3.6 The Agency's DSAP and PoT requirement

The Agency's requirement to appoint DSAPs and PoTs comes from an assessment of the operating environment by the Agency Security Adviser, and the real need for staff to hold a clearance above that of a Baseline level. The following table sets out the Clearance level for personnel within the Agency.

DSAP	
Security Clearance Level	**Agency Position**
Positive Vetting Negative Vetting Level 2 (NV2) Negative Vetting Level 1 (NV1)	No identified requirement for positions to access CONFIDENTIAL, SECRET, and TOP SECRET assets and information.

Note: DSAP only relates to the National Security clearance levels of NV1, NV2 and Positive Vetting.

PoT	
Security Clearance Level	**Agency Position**
Baseline Vetting	• Agency Head • Security Executive • Agency Security Adviser (ASA) • Information Technology Security Adviser (ITSA) • All Senior Executive Service (SES) • Agency Personnel (as required)
Dissemination Limiting Marker (DLM)	The majority of Agency information holdings are at a DLM level (excluding Sensitive Cabinet). The DLM level of information does not require a formal security clearance, but is subject to the 'need-to-know' principle. All Agency staff are required to fulfil an identity check and a police criminal history check before engagement.

5. *Administration and Review of this Guideline*

4.1 Review of this Guideline

This guideline will be reviewed **annually** by the Agency Security Adviser for currency and updated if required.

4.2 Administration of this Guideline

The Agency Security Adviser is responsible for the administration and review of this guideline.

6. *Other Documents Applicable to this Guideline*

5.1 Applicable Documents

- Agency Security Plan
- Agency Security Policy
- Australian Government Personnel Security Protocol
- Australian Government Personnel Security Guidelines
- Austraian Government Security Vetting Agency SVA 003