People Security

PESEC-1:
Recruiting the right people

Department of Premier and Cabinet

Tasmanian Government

Contents

Author: Resilience and Recovery Tasmania
Publisher: Department of Premier and Cabinet
Date: April 2023

About this document

This document – PESEC-1: Recruiting the right people – is part of a suite of policies and guidance developed to assist Tasmanian Government agencies to meet requirements under Tasmania's Protective Security Policy Framework (TAS-PSPF).

The TAS-PSPF is a whole-of-government approach to the protection of Tasmanian Government information, people and assets from compromise and harm. It establishes minimum protective security standards and makes clear that to continue ensuring the security of our people and assets, Tasmanian Government agencies need to:

- understand the security environment in which they operate
- identify and understand the most critical assets they must protect
- mitigate security vulnerabilities on a prioritised security-risk basis
- anticipate and prepare for emerging security trends which threaten their ability to effectively undertake government business functions
- continue to improve protective security practices through accountability and governance.

The TAS-PSF sets out 14 core requirements – with each accompanied by supplementary requirements – that define what must be addressed in order to protect our information, people and assets.

The suite of policies and guidance, including those found in this document, ensures that the TAS-PSPF will be applied across Tasmanian Government agencies in a consistent way. It will also assist agencies to achieve the expected outcomes of the following protective security domains under the TAS-PSPF:

- security governance
- information security
- people security
- physical security.

The table below lists all 14 core requirements of the TAS-PSPF and their corresponding policies. The name of the policy and guidance provided in this document is highlighted.

Protective security outcome	Core requirement	Relevant policies and guidance
Security governance	1	GOVSEC-1: Establish security governance
	2	GOVSEC-2: Security advice and responsibilities
	3	GOVSEC-3: Security awareness
	4	GOVSEC-4: Annual reporting
	5	GOVSEC-5: Security planning
	6	GOVSEC-6: Reporting incidents and security investigations
Information security	7	INFOSEC-1: Access to, and management of, official information
	8	INFOSEC-2: Protecting official information
	9	INFOSEC-3: Robust technology and information systems
People security	10	PESEC-1: Recruiting the right people
	11	PESEC-2: Ongoing suitability assessment
	12	PESEC-3: Managing separating people
Physical security	13	PHYSEC-1: Protecting assets
	14	PHYSEC-2: Agency facilities

Definitions and shortened terms

Guiding term	What this means in the context of the TAS-PSPF
must/will/ required/ responsible for	Any of these terms refer to an essential action that all agencies and Accountable Authorities must take.
must not	This term refers to an action that is prohibited – agencies and Accountable Authorities must NOT take this action.
should/ recommended	Either of these terms refer to an action that agencies and Accountable Authorities ought to take as best practice, unless justifiable circumstances exist.
should not	This term refers to an action that agencies and Accountable Authorities ought to avoid, unless justifiable circumstances prevent an alternative action.
may	This term refers to an action that is optional to agencies and Accountable Authorities.

Term	What this means in the context of the TAS-PSPF
Accountable Authority/ies	The person or people responsible for, and with control over, a Tasmanian Government public authority. This includes, but is not limited to, agencies (as defined in the *State Service Act 2000*), administrative units, bodies corporate, statutory authorities, and instrumentalities of the Crown.
agency/ies	A Tasmanian Government agency/department or sub-entity.
Agency Security Advisor	Person/people nominated to perform security functions or specialist services related to security within an agency. This role supports the Accountable Authority in security monitoring and compliance.
ASIO Outreach	ASIO's public-facing website, which provides advice to government, industry and academia on current and emerging security threats and security policy, available by subscription.
asset	An agency's people, information, and physical items, including ICT systems, technology and information infrastructure.
availability	Ensuring that authorised users have access to information and associated assets when required.
classification	A process that determines and stipulates the extent of protection required to prevent information from compromise and harm.

Term	What this means in the context of the TAS-PSPF
compromise	May include exposure to loss and unintended or unauthorised access, misuse, information disclosure and intrusion of business activities and information. Compromise is a risk and hindrance to business delivery, safety and security.
confidentiality	Ensuring that information is accessible only to those authorised to have access and a 'need to know'.
consequence	The outcome, or expected outcome, of any compromise of information or a security incident.
contractor	External or third party contracted to provide services to an agency. For the purpose of the TAS-PSPF, contractor includes sub-contractor and service provider.
core requirement	A requirement that agencies must meet to achieve the government's desired protective security outcomes. Each of the 14 TAS-PSPF policies includes a core requirement (as well as supplementary requirements).
employees	All people conducting work on an agency premises, including contractors. See also, people.
function	The purpose or role of an agency.
handling	Any processes for accessing, transmitting, transferring, storing or disposing of protected information.
integrity	Safeguarding the accuracy and completeness of information and processing methods, i.e. information has been created, modified or deleted by the intended authorised means and is correct and valid.
official information	All Tasmanian Government documents, intellectual property and information that is held, transmitted or obtained by an agency.
originator	The instigating individual (or agency) responsible for producing information.
outcomes	The protective security 'end-state' aims of the Tasmanian Government relating to 4 security domains: governance, information, people and physical.
people	Employees and contractors, including secondees and any service providers that an agency engages. It also includes anyone who is given access to Tasmanian Government assets.

Term	What this means in the context of the TAS-PSPF
principles	Fundamental values that guide decision-making. There are 5 principles that inform protective security settings in the TAS-PSPF. 1. Security is a responsibility of government, its agencies and its people. 2. Each agency is accountable and owns its security risks. 3. Security will be guided by a risk management approach. 4. Strong governance ensures protective security is reflected in agency planning. 5. A positive security culture is critical.
protected information	Information which has been assessed and classified as requiring protective markings and protection.
protection	The processes and procedures applied to ensure the confidentiality, integrity and availability of information and assets.
protective marking	The level of classification applied to information, and any other handling instructions or protections the information requires due to the level of harm should it be compromised.
PSPF maturity rating	The level to which an agency has addressed and implemented the core and supplementary requirements in the TAS-PSPF.
risk appetite	The risk an agency or Accountable Authority is willing to accept.
risk tolerance	The level of risk an agency is comfortable taking after risk treatments have been applied to achieve an objective or manage a security risk.
security culture	The characteristics, attitudes and habits within an organisation that establish and maintain security.
security incident	A security incident is: • an action, whether deliberate, reckless, negligent or accidental, that fails to meet protective security requirements or agency-specific protective security practices and procedures which results, or may result in, the loss, damage, corruption or disclosure of information or assets • an approach from anybody seeking unauthorised access to protected assets • an observable occurrence or event (including natural or man-made events) that could harm Tasmanian Government information, people or assets.
security maturity	The measure of an agency's ability to manage their security risks within their risk environment and aligned to their risk tolerances.
security plan	Central document detailing how an agency plans to manage and address their security risks.

Term	What this means in the context of the TAS-PSPF
security risk	Something that could result in compromise, loss, unavailability or damage to information or assets, or cause harm to people.
security risk management	Managing risks related to an agency's information, people and assets.
security vetting	An authorised vetting agency's assessment of a clearance subject's suitability to hold a security clearance.
sensitive	Information classified as sensitive is not protected information; however, this information requires some protections on a 'needs to know' basis.
supplementary requirements	The actions needed to implement the TAS-PSPF core requirements and attain the government's desired protective security outcomes. Each of the 14 core requirements includes supplementary requirements to help implement the TAS-PSPF.
threat	The intent and capability of an adversary.
threat actor/adversary	An entity that is partially or wholly responsible for an incident that impacts – or has the potential to impact – an agency's security.
visitor	Any person who attends an agency and/or has access to its assets, who is not employed or otherwise engaged by that agency.
vetting	The evaluation of a person's suitability to obtain and maintain a security clearance and access sensitive and protected assets.
zone	The physical locality, workspaces, and design of areas within an agency that store assets and information, specifically where information is produced, accessed, handled and stored. Security zoned areas range from 1-5, where the security requirements increase with the applicable zone number allocation.

Acronym/abbreviation	Meaning
ICT	information and communication technology
AGSVA	Australian Government Security Vetting Agency
SMSMP-PVG	Sensitive Material Security Management Protocol – Personnel Security – Positive Vetting Guidelines

Context

The **PESEC-1: Recruiting the right people** policy and guidance will assist agencies to achieve an effective protective security outcome within the people security domain of the TAS-PSPF. They address core requirement 10 and its supplementary requirements.

Core requirement 10

Accountable authorities must assess the initial suitability, and validate the identities, of people who have access to, or are seeking access to, Tasmanian Government assets.

Supplementary requirements

To determine that the agency is recruiting the right people, the Accountable Authority will:

a) conduct pre-employment screens in accordance with any statutory requirements and limitations, which may include:[1]

   a. verification of identity and eligibility

   b. reference checks, as necessary, to ensure a person's suitability to access Tasmanian Government assets.

b) identify specific roles and positions which may require additional certifications/checks, which may include:[2]

   a. working with vulnerable people

   b. drug and alcohol testing

   c. relevant police checks

   d. psychometric testing

   e. security clearances.

Access to Tasmanian Government assets need to be protected. Agencies must apply a risk-based approach to employment processes, ensuring the suitability of its people, and external providers, to access these assets. The TAS-PSPF describes how the suitability and validation of agency people should be applied through pre-employment screens and security vetting where required.

[1] This will be based on the type of engagement and the agency, along with any relevant state-based award/agreement and legislation.

[2] If such action is identified as necessary, seek appropriate approvals for the associated statement of duties and/or advertising.

Guidance

Introduction

The purpose of people security measures is to validate the identity of individuals (agency people) and provide a level of assurance as to their honesty, integrity and reliability.

You must ensure all people performing work for your agency who access Tasmanian Government information and assets:

- are suitable for the purposes of granting access
- have the right to work in Australia
- have their identity validated
- agree to comply with government and agency policies, standards, protocols and requirements that protect information, people and assets from compromise and harm.

You should minimise risk by having effective recruitment processes and strategies in place.

Required action: Conduct pre-employment screens

The TAS-PSPF requires Accountable Authorities to own the security risks of their agency, which includes the responsibility to identify and manage the risks associated with recruiting people into the agency.

Pre-employment screening is the primary activity you can employ to mitigate people security risks. It is a process which ensures the eligibility and suitability of the people engaged to work in your agency. In accordance with Employment Direction 7-2013,[3] you must first obtain approval from the Head of the State Service to conduct pre-employment checks.[4] When you have that approval from the Head of the State Service, you must then list the relevant pre-employment checks in the job advertisement under 'essential requirements' in the statement of duties.

The level of pre-employment screening required will vary according to your agency's context, risk environment and the position being filled. You must manage the people security risks associated with each role within your agency. To do this, consider the essential responsibilities and duties of

[3] For further information about Employment Direction 7-2013, please refer to the Department of Premier and Cabinet website at www.dpac.tas.gov.au/divisions/ssmo/employment_directions

[4] If checks are made without necessary approval and action is taken on the information obtained to preclude a person from employment, then that person may initiate a complaint where such action is seen to be inappropriate or discriminatory.

the position, identify any risks associated with these responsibilities and duties, and decide on the screening you will apply to limit these risks.

In support of holistic agency policies and procedures, it is recommended that you carry out minimum pre-employment checks on all potential employees, including existing employees who are changing roles, contractors, short-term staff, and secondees.

Completing pre-employment screening prior to engagement is particularly important for positions where a security clearance has been identified as necessary. If someone is found to be unsuitable during pre-employment or agency-specific screening, this means they are not suitable for a security clearance and so you must not seek a security clearance for these individuals.

To enhance recruitment methods in your agency, you should have a strategy and implement processes for responding to concerns which may arise from:

- pre-employment screening checks
- ongoing suitability checks.

Privacy

Agencies must ensure all pre-employment screening checks are conducted in line with the *Personal Information Protection Act 2004*.

It is recommended that your agency obtains informed consent, from all applicants who are applying for positions with your agency, for you to collect, use and disclose personal information (including sensitive information) for the purposes of reviewing their eligibility and suitability for employment. This can be strengthened through the provision of a privacy statement in any recruitment and pre-employment paperwork.

You may use statutory declarations to confirm that any information provided is truthful.

It is important to note that, when you collect any personal information throughout a recruitment process, you must protect such information. Due to the nature of personal information, it must be protectively marked OFFICIAL: Sensitive and in some circumstances may require a security classification.[5]

[5] For further information on protecting information and applying security classifications, refer to TAS-PSPF policy: Protecting official information (INFOSEC-2).

Identity and eligibility checks

Identity checks are an important element of any pre-employment screening process. People may present inaccurate or incomplete identity information to conceal a history of criminal activity, misconduct or poor work performance to obtain a role they should not occupy.

You should consider performing identity checks at multiple stages throughout the recruitment process or on promotion. It is recommended that you perform a 100-point check[6] on all applicants chosen for progression.

An eligibility check ensures that an individual is eligible to work in Australia by confirming either the individual's Australian citizenship, or a valid work visa. You should check visa conditions for applicants who are not Australian citizens to determine whether the conditions allow them to perform the job they are applying for.

Reference checks

It is recommended that you conduct reference checks to determine a person's quality, integrity and suitability by verifying past performance in employment, including conduct and behaviour.

Referees should be from a legitimate source and free from any conflicts of interest. Referee checks must obtain information from someone who has direct knowledge of the applicant's experience and should cover a period of at least the previous 3 months.

Where appropriate, information relating to the following may be sought from the nominated referee:

- any substantiated complaints about a person's behaviour
- information in relation to any action, investigation or inquiry concerning the person's conduct, character or competence
- security-related issues that might reflect on the person's integrity and reliability.

[6] A 100-point check makes it harder for people to use a false identity because multiple identity documents are required from specific categories. For example, a candidate may be required to submit one or more primary documents such as a birth certificate or passport, and one or more secondary documents such as a driver's licence or Medicare card.

The table below outlines some recommended pre-employment screening checks.

Screening check	Rationale
Employment history check	Identifying unexplained gaps or anomalies in a person's employment. A person may not disclose period/s of employment which may have ended in termination or where a poor referee report is anticipated. A history of short employment may indicate poor reliability. Where possible, employment history should be checked with former employers. If this isn't possible, then the information should be sourced through referee checks. It is recommended that, where applicable, an employment history of 5 years is confirmed.
Residential history check	A residential history check helps substantiate a person's identity in the community. Evidence of a person's current permanent residential address should be sought. It is recommended that residential history checks for newly engaged people cover a period of 5 years. Where applicable, you should consider whether the person's explanation about periods of residency for which they cannot provide supporting documents is reasonable.
Credit history check	A credit history check helps establish if a person has a history of financial defaults, if they may be in a difficult financial situation, or other concerns regarding their finances. These situations potentially increase a person's vulnerability to financial incentives. Credit history checks can be obtained through an accredited financial credit check organisation on a fee-for-service basis.
Qualification check	Qualification checks verify a person's qualification with the issuing institution. You may undertake qualification checks with the issuing institution, as well as any professional associations or memberships that are a requirement of the role the person would be performing.
Conflict of interest declaration	Conflict of interest declarations identify conflicts, real or perceived, between a person's employment and their private, professional or business interests which could influence the performance of their duties, including the ability to protect Tasmanian Government information and assets. Conflicts of interest could include financial particulars, secondary employment, and associations. The Tasmanian State Service Code of Conduct (*State Service Act 2000* – Section 9) requires employees to disclose any conflict of interest in connection with their employment.

Agency-specific checks	It is recommended that you consider and implement any additional pre-employment checks that are in line with your agency's operational functions and needs where the people security risks identified are not mitigated by the previously listed screening checks. These additional screening checks may include: • psychometric testing • drug and alcohol testing • more detailed financial probity checks. Any such action by your agency will require legal consideration and advice as necessary.
Other screening requirements	Some roles in the Tasmanian Government may already necessitate specific screening requirements, which include a working with vulnerable people registration.

Table 1 – Recommended pre-employment screening checks

Required action: Identify positions requiring additional screening

When you identify duties and positions with an increased security risk, additional certifications and pre-employment checks may be required. The additional checks you apply will depend on several factors including the security context and culture, as well as the operating environment of your agency.

In some circumstances, a position may not have sustained increased security risk associated with it; however, your agency may identify specific duties of the position which subject the occupant to times of heightened risk. In these circumstances, it may be warranted to conduct additional screening or checks.

Examples of roles that may require additional checks are:

- child-related employment
- disability services employment
- aged-care sector employment
- roles which involve working in sensitive and protected areas
- roles which directly affect the safety of other people.

Additional checks may include:

- working with vulnerable people registration
- drug and alcohol testing
- relevant national police check
- psychometric testing
- security clearances.

When you have identified a position requiring additional pre-employment screening or checks, you should establish accurate expectations by outlining those requirements in the statement of duties.

Where a position requires a national security clearance, this should be included in the statement of duties in the advertisement. More information about security clearances is provided below.

Contractors

You should be mindful of security risks associated with contractors (including sub-contractors). It is recommended that, to protect your information, people and assets, you apply the same security measures to contractors as you would with other employees.

The same security measures must also apply where recruitment of contractors occurs through an employment (or other) agency. A signed agreement between you and the employment (or other) agency must specify their responsibilities for conducting pre-employment checks and the notification procedures to be followed where there is cause for doubt or concern.

It is recommended that contractors are re-screened if your agency is planning on renewing or extending a contract to identify new risks arising from changes in the work environment or the contractor's personal circumstances.

Volunteers

The term 'volunteering' covers a wide range of activities in society. It includes formal volunteering that takes place within organisations in a structured way, as well as informal volunteering – acts that take place outside of a structured volunteer process.

Your agency is required to implement a consistent approach to the management and support of all volunteers. It is recommended that you implement screening processes which detect any persons who may be unsuitable to act as volunteers, including any checks mandated by legislation.

You should develop volunteering policies specific to your agency's needs and update these regularly, so they remain contemporary. There are specific requirements under the *Registration to*

Work with Vulnerable People Act 2013 for screening volunteers working with vulnerable members of the Tasmanian community.

Working with vulnerable people registration

Working with vulnerable people registration is an ongoing assessment of a person's eligibility to work with vulnerable people and involves a check of a person's national criminal history and other disciplinary and police information.

In accordance with the *Registration to Work with Vulnerable People Act 2013,* registration is required for persons who participate in the following:

- child-related activity
- vulnerable adult-related activity
- child and vulnerable adult-related (NDIS endorsed) activity
- a category of activity or service prescribed by the regulations as a category of registration.

Drug and alcohol testing

The inclusion of drug and alcohol testing will depend on your agency's work activity, and the health and safety or reputational risks. Such testing may be considered reasonable where it is conducted with a view to protecting the safety of your people, clients or the public. If your agency identifies drug and alcohol testing as a requirement, you should develop and implement an agency policy that clearly sets out the procedure to be followed for alcohol and drug testing.

If adopting drug and alcohol testing, you must declare any relevant pre-employment or ongoing testing requirements in the job advertisement and statement of duties to ensure applicants are aware of this.

Relevant police checks

A national police check involves a search of a person's name against the criminal history records held by police services Australia-wide, to determine any matches to previous criminal convictions. Identifying the inherent requirements of a position will help you decide whether a police check is warranted; if you do decide a check is warranted, you must be clear about which convictions would preclude an applicant.

Where you determine that a national police check is required, you must communicate this in the advertisement and statement of duties for the position. In these circumstances, it is strongly recommended that you request a copy of a valid national police check from applicants as part of their pre-employment screening process.

National police checks can be conducted by Tasmania Police and the Australian Federal Police on a fee-for-service basis.[7]

Psychometric assessments

Psychometric assessments can be used to measure a person's aptitude and suitability to meet the requirements of a position. There may be situations when conducting psychometric assessment is appropriate for your agency to use in pre-employment processes, which may include for positions or promotions where certain characteristics or aptitude are required and may be difficult to assess in other pre-employment screens and interviews.

Examples of psychometric assessments include:

- cognitive ability assessments
- numerical reasoning
- verbal reasoning
- abstract reasoning
- personality questionnaires.

The assessments used by your agency should be fit-for-purpose,[8] which means the person responsible for, or facilitating, the recruitment process understands the purpose of the chosen assessment and how the results will be used.

If your agency adopts psychometric assessments in recruitment processes, they should be used to inform decisions throughout selection but should not be the sole factor in determining suitability. They may also be used to inform onboarding activities, ongoing management, and development plans for suitable applicants.

[7] For checks conducted by Tasmania Police, refer to www.police.tas.gov.au/services-online/police-history-record-checks/ ; for checks conducted by the Australian Federal Police, refer to www.afp.gov.au/what-we-do/national-police-checks

[8] Fit-for-purpose assessment methods are those that are well suited to what is being assessed, in the particular context it is being assessed.

Security clearances

The conduct of Tasmanian Government business requires sharing of information that is highly sensitive and/or security-classified. This sharing requires your agency to have suitably security-cleared people who can assess and handle the information – including the Accountable Authority.

It is important to note that security clearances are not obtainable on an individual basis; they are only applied for in circumstances where a person performs a role where they are expected to have access to security-classified information. This includes positions involved in a workflow where the person/s are involved in the handling of documents, system administration and have access privileges to such information or assets.

You may also identify positions where a security clearance is required to provide a higher level of assurance about a person's suitability.[9] Additionally, positions in your agency may require an occupant to access particular information or assets necessitating a security clearance, for example, specific information or physical locations within your agency (security zoned areas) and/or specific information and communication technology (ICT) systems.

When you have identified the positions in your agency requiring a security clearance, you must maintain a record which identifies those positions and the level of clearance required. It is recommended that this register includes the following:

- positions requiring a security clearance for ongoing access to security-classified information/assets
- positions requiring a higher level of assurance than can be obtained through pre-employment or agency-specific screening
- occasions when the requirement for the security clearance will be reassessed (i.e. when the position becomes vacant, position reclassification, promotion).

It is the responsibility of your agency to ensure each person working in an identified position has a valid security clearance issued by an authorised vetting agency.

The following table indicates the level of security clearance required for each security classification.

[9] Such positions may involve the occupant having access to aggregations of information or assets, or due to the nature of the role e.g. fraud mitigation or anti-corruption.

Clearance level	Ongoing access provisions	Level of conditional access
Not required. Pre-employment screening is sufficient.	OFFICIAL: Sensitive	N/A
Baseline **(B)**	Classified resources up to and including **PROTECTED**	N/A
Negative Vetting Level 1 **(NV1)**	Classified resources up to and including **SECRET**	NV1 security clearance holders can be provided with temporary access to TOP SECRET classified resources in certain circumstances.
Negative Vetting Level 2 **(NV2)**	Classified resources up to and including **TOP SECRET**	An NV2 security clearance will be sufficient for most roles requiring intermittent access to TOP SECRET classified resources.
Positive Vetting **(PV)**	Classified resources up to and including **TOP SECRET**, including some caveated information	PV clearances should only be sought where there is a demonstrated need to access extremely sensitive information, capabilities, operations and systems. Agencies should first consider whether an NV2 clearance would meet the position's requirement for a security clearance.

Table 2 – Security clearance access provisions

Security clearance exemptions

There are some Tasmanian Government office holders who, only while exercising the duties of the office, are exempt from holding a security clearance for the purpose of accessing security-classified information. Details can be found in TAS-PSPF policy: Access to, and management of, official information (INFOSEC-1). These exemptions do not apply to any staff of named office holders.

Eligibility for a security clearance

To be eligible for an Australian Government security clearance, it is a requirement that an applicant is an Australian citizen, and they must have a checkable background.[10] There are times when citizenship and checkable backgrounds may be waived; however, this requires you to demonstrate there is an exceptional business requirement and that you have conducted an appropriate risk assessment. In these circumstances, the authorised vetting agency may still deny such application where there are concerns about the person's suitability which cannot be mitigated, including any concerns relating to the eligibility waiver.

The risk assessment for a citizenship or checkable background waiver must be based on the position, the applicant, and the agency. If a security clearance is issued under either of these waivers, it is not transferable unless the exceptional business requirement and risk assessment provision are undertaken and accepted for the new position or agency.

The table below provides details regarding exceptional business requirements and risk assessments.

Eligibility waiver component	**Requirement**
Exceptional business requirement	It is recommended that you consider the following questions before establishing an exceptional business requirement: • Is the role critical to meeting your agency's outcomes? • Can the role be performed by a person who does meet the eligibility requirements? • Can the role be redesigned to remove the requirement to access classified information or assets, thereby restricting access to those who already hold or are eligible to hold the appropriate security clearance?
Risk assessment	You must conduct security risk management in accordance with the suite of TAS-PSPF security governance policies. When conducting a risk assessment for an eligibility waiver, it is recommended that you also consider: • potential conflicts of interest • advice from the authorised vetting agency and ASIO, including –

[10] A checkable background is where an authorised vetting agency is able to complete the minimum vetting checks and inquiries for the required duration and these provide adequate assurances regarding the individual's life or background for the level of clearance required.

	○ details of security concerns associated with the applicant's uncheckable background and assessment of the impact of this uncheckable period against the whole-of-person assessment ○ any known concerns[11] about the applicant ○ any threat assessments from ASIO on the applicant's country/ies of citizenship or the country/ies that give rise to any uncheckable periods ○ consultation with third parties whose information, people and assets may be accessed by the applicant and especially the originating or controlling agency of any TOP SECRET information and assets and any foreign entities.
	• for citizenship waivers – ○ details of the applicant's visa status and whether they are actively seeking Australian citizenship, or plan to ○ your agency's plan to ensure the applicant does not access caveated AUSTEO[12] information ○ any threat assessments from ASIO on the applicant's country/ies of citizenship or the country/ies that give rise to any uncheckable periods ○ consultation with third parties whose information, people and assets may be accessed by the applicant and especially the originating or controlling agency of any TOP SECRET information and assets and any foreign entities. • the period to be covered by the waiver • proposed risk mitigations, including any conditions placed on the applicant subject to the waiver.

Table 3 – Eligibility waiver – exceptional business requirements and risk assessments

Recognising existing security clearances

There may be circumstances where people in your agency hold, or have previously held, a security clearance issued by an authorised vetting agency.[13] If this occurs, your agency may elect to sponsor that security clearance. You should identify if a prospective employee has or ever previously held a security clearance prior to seeking and sponsoring a new clearance.

[11] For example, any recent changes in behaviour or circumstances or finances, which cause you a level of concern as to the suitability of the person to gain a security clearance.

[12] For information on caveats, please see TAS-PSPF policy: Protecting official information (INSFOSEC-2)

[13] Including security clearances issued by a state or territory government (e.g. Tasmania Police) 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.

There are circumstances where a security clearance cannot be recognised, as follows:

- the security clearance has expired due to the period since the clearance was granted or last revalidated exceeding –
    - Baseline (B) – 15 years
    - Negative Vetting 1 (NV1) – 10 years
    - Negative Vetting 2 (NV2) – 7 years
    - Positive Vetting (PV) – 7 years or if an annual security clearance has not been completed in the previous 2 years, the Sensitive Material Security Management Protocol – Personnel Security – Positive Vetting Guidelines (SMSMP-PVG) also requires an annual security appraisal to have been completed within the last 2 years.[14]
- the authorised vetting agency has concerns that the clearance holder is no longer eligible or suitable to access security-classified information and assets at the relevant clearance level
- the clearance was granted on the basis of an eligibility (citizenship or background) waiver
- the clearance was granted subject to clearance conditions
- the clearance has ceased.

If a security clearance is subject to an eligibility waiver or clearance conditions, the authorised vetting agency will advise the new sponsoring agency. For clearances subject to an eligibility waiver, the new sponsoring agency will be required to accept and undertake the exceptional business requirement and risk assessment provisions prior to requesting transfer of sponsorship. If the clearance is subject to conditions, the new sponsoring agency is required to accept the clearance conditions.

Authorised vetting agencies

You must use the Australian Government Security Vetting Agency (AGSVA) to conduct vetting, or where authorised,[15] conduct security vetting in a manner consistent with the personnel security vetting standards.[16]

State and territory governments may request AGSVA to conduct security vetting up to and including Negative Vetting 2, when sponsored by an appropriate government agency.[17]

---

[14] The SMSMP-PVG is available via GovTEAMS, where users are required to register for an account and request access to the Protective Security Policy community.

[15] Tasmania Police is an authorised vetting agency and clearance sponsor for Tasmania Police employees.

[16] Located in the Australian Government Protective Security Policy Framework policy 12: Eligibility and suitability of personnel.

[17] The Australian Government and state and territory government agencies are authorised to sponsor an AGSVA clearance, not individuals. For further information, please contact Resilience and Recovery Tasmania via sem@dpac.tas.gov.au

Minimum security checks

The Australian Government Protective Security Policy Framework outlines the minimum security checks required for a security clearance applicant and any additional checks that may be required for each level of security clearance.

Conditional security clearances

If there is any information of security concern identified throughout the vetting process that of itself is not sufficient to deny a security clearance, those risks may be managed through the application of conditions to the clearance.

Where this eventuates, before the clearance is issued, the sponsoring agency's Accountable Authority, or Chief Security Officer, and the clearance applicant must agree to the conditions associated with the clearance. Non-compliance with conditions may be a trigger for review.

Sharing information of security concern

Throughout the vetting process, there may be information of security concern identified by the authorised vetting agency. If this occurs, the vetting agency must advise the sponsoring agency at the same time as advising the outcome of the security clearance application. This may include information such as vulnerabilities or risk factors and risk mitigation strategies applied by the vetting agency. By sharing this information, the sponsoring agency can understand and manage any risks relating to the clearance holder's ongoing access to Tasmanian Government information and assets.

For more detailed and further information regarding security clearances, including the requirements of authorised vetting agencies, please refer to the Australian Government Protective Security Policy Framework policy 12: Eligibility and suitability of personnel.

References and resources

Australian Government, security clearances, at www.defence.gov.au/security/clearances
Australian Government, Protective Security Policy Framework, at www.protectivesecurity.gov.au/publications-library/policy-12-eligibility-and-suitability-personnel
New Zealand Government, Protective Security Requirements, at www.protectivesecurity.govt.nz/personnel-security/managing-insider-risk/recruiting-the-right-person/
New Zealand Government, Employment New Zealand, at www.employment.govt.nz/workplace-policies/tests-and-checks/drugs-alcohol-and-work/
SA Government, personnel security, at www.security.sa.gov.au/documents/SAPSF-PERSEC1-Recruiting-employees-B451679-2.pdf
Standards Australia, AS 4811:2022 Workforce screening
Victorian Government, Victorian Protective Data Security Standards, at https://ovic.vic.gov.au/wp-content/uploads/2021/02/20210216-VPDSS-V2.0-Implementation-Guidance-V2.1.pdf

Department of Premier and Cabinet
Resilience and Recovery Tasmania

Phone:

(03) 6232 7979

Email:
sem@dpac.tas.gov.au