12 Eligibility and suitability of personnel

A. Purpose

1. This policy details the pre-employment screening processes and standardised vetting practices to be undertaken when employing personnel and contractors. These processes provide a high-quality and consistent approach to managing personnel eligibility and suitability risk across government.

B. Requirements

B.1 Core requirement

Each entity must ensure the eligibility and suitability of its personnel who have access to Australian Government resources (people, information and assets).

Entities must use the Australian Government Security Vetting Agency (AGSVA) to conduct vetting, or where authorised, conduct security vetting in a manner consistent with the Personnel Security Vetting Standards.

2. Pre-employment screening is the primary activity used to mitigate an entity's personnel security risks. Entities may use security clearances where they need additional assurance of the suitability and integrity of personnel. This could be for access to security classified information, or to provide greater assurance for designated positions.

B.2 Supporting requirements

3. The supporting requirements clarify conditions for pre-employment screening and security clearances. This includes outlining the respective responsibilities of sponsoring entities and authorised vetting agencies in relation to security clearances.

Supporting requirements for eligibility and suitability of personnel

#	Supporting requirements
Requirement 1. Pre-employment screening	Entities **must** undertake pre-employment screening, including: a. verifying a person's identity using the Document Verification Service b. confirming a person's eligibility to work in Australia, and c. obtaining assurance of a person's suitability to access Australian Government resources, including their agreement to comply with the government's policies, standards, protocols and guidelines that safeguard resources from harm.
Requirement 2. Security clearances	Entities **must**: a. identify and record positions that require a security clearance and the level of clearance required b. ensure each person working in an identified position has a valid security clearance issued by an authorised vetting agency c. before seeking a security clearance, confirm that the person meets pre-employment screening requirements [Note i] and is an Australian citizen d. if the person is not an Australian citizen and has a valid visa with work rights, provide the authorised vetting agency with an eligibility waiver by:

#	Supporting requirements
	i. establishing an exceptional business requirement and conducting a risk assessment, and ii. asking the accountable authority to consider and accept the risk of waiving the citizenship requirement. Note ii e. if the authorised vetting agency assesses that the person has an uncheckable background, provide the vetting agency with an eligibility waiver by: i. establishing an exceptional business requirement and conducting a risk assessment (including seeking the advice of the vetting agency), and ii. asking the accountable authority to consider and accept the risk of waiving the checkable background requirement. Note iii
Requirement 3. Personnel security vetting standard	Authorised vetting agencies **must**: a. only issue a security clearance where the clearance is sponsored by an Australian Government entity or otherwise authorised by the Australian Government b. 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 c. assess the clearance subject's eligibility and suitability to hold a security clearance by: i. considering their integrity (ie the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) in accordance with the Personnel Security Adjudicative Guidelines (at **Annex A**) ii. conducting minimum personnel security checks for a security clearance outlined below, and iii. resolving any doubt in the national interest.

Minimum personnel security checks

Check	Security Clearance Level			
	Baseline Vetting	**Negative Vetting 1**	**Negative Vetting 2**	**Positive Vetting**
Identity check	✓ Required	✓ Required	✓ Required	✓ Required
	Entities must verify the person's identification documents with the issuing authority by using the Document Verification Service for Australian issued primary identification documents.			
Confirmation of Australian citizenship and status of any other citizenships	✓ Required	✓ Required	✓ Required	✓ Required
Background assessment	✓ Required for the checkable period of 5 years	✓ Required for the checkable period of 10 years	✓ Required for the checkable period of 10 years	✓ Required for the checkable period that is greater of 10 years or from the age of 16
Official secrets declaration	✓ Required	✓ Required	✓ Required	✓ Required
Statutory declaration	✓ Required	✓ Required	✓ Required	✓ Required
Referee checks	✓ Required	✓ Required	✓ Required	✓ Required
Digital footprint check	✓ Required	✓ Required	✓ Required.	✓ Required
National police check	✓ Required, no exclusion	✓ Required, full exclusion	✓ Required, full exclusion	✓ Required, full exclusion
Financial history assessment	✓ Required	✓ Required	✓ Required	✓ Required
Financial statement	Not required	✓ Required	✓ Required	✓Required with supporting documents
Financial probity assessment	Not required	Not required	Not required	✓ Required
ASIO security assessment	Not required	✓ Required	✓ Required	✓ Required
Security interview	Not required	Not required	✓ Required	✓ Required

#	Supporting requirements				
	Psychological assessment	Not required	Not required	Not required	✓ Required

Requirement 3. (continued)

d. if a clearance subject has an uncheckable background:
   i. provide the sponsoring entity with information to inform a risk assessment, and
   ii. only issue a clearance if the accountable authority waives the checkable background requirement (see **Requirement 2e**)
e. if security concerns are identified during the vetting or security assessment process that are not sufficient to deny a security clearance, and the related risks can be managed through conditions attached to the security clearance:
   i. identify the clearance conditions
   ii. provide the sponsoring entity with information about the security concerns to inform a risk assessment, and
   iii. only issue a conditional security clearance if the accountable authority and the clearance subject accept the clearance conditions [Note iv]
f. if any other relevant information of security concern is identified during the vetting process, provide the sponsoring entity with information to inform a risk assessment when advising them of the outcome of the security vetting process [Note v]
g. without compromising the national interest, 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, [Note vi] and
h. ensure all vetting personnel attain and maintain the required skills and competencies for their role.

Supporting requirements notes:

[i] An exception applies for entities authorised as vetting agencies.
[ii] The accountable authority may delegate this decision to the Chief Security Officer.
[iii] The accountable authority may delegate this decision to the Chief Security Officer.
[iv] The accountable authority may delegate this decision to the Chief Security Officer, however the Chief Security Officer is required to notify the accountable authority of the clearance conditions.
[v] Where security concerns are identified that may lead to an adverse recommendation, the vetting agency (while any determination is still pending, including where a clearance subject has been invited to respond to identified risks) shares only relevant information with the sponsoring entity to enable temporary mitigations until a final outcome is made. See Requirement 3g.
[vi] Separate arrangements ensure procedural fairness and national security are preserved where denial of a clearance is based on an ASIO security assessment.

4. **Requirement 1** applies to all personnel; this includes security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources. **Requirements 2** and **3** apply to security cleared personnel only.

C. Guidance

C.1 Pre-employment screening

5. Pre-employment screening includes:
   a. mandatory and recommended pre-employment checks applied to provide a level of assurance about the individual's suitability to access Australian Government resources
   b. entity-specific checks to mitigate security threats applicable to the entity that are not addressed by minimum pre-employment screening.
6. The Attorney-General's Department recommends that entities conduct and finalise pre-employment and entity-specific screening after the conclusion of the merit selection process but 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.

7. Completing screening prior to engagement is particularly important for positions that have been identified as requiring a security clearance. If an individual is found to be unsuitable as part of the pre-employment and entity-specific screening, entities must not seek a security clearance for the individual (see **Requirement 2c**).

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

9. For entities authorised as vetting agencies, pre-employment screening may be conducted concurrently with security vetting to permit streamlined engagement of personnel. The Attorney-General's Department recommends that entities conducting concurrent pre-employment screening and security vetting record determinations against the criteria identifying whether a decision relates to an employment screening threshold or a security clearance threshold.

10. For personnel transferring within the Australian Government, some pre-employment screening checks may have already been conducted. The Attorney-General's Department recommends confirming if checks have already been undertaken by the losing entity. Additional checks can be done to meet the specific entity employment requirements of the gaining entity or if the check needs to be revalidated (see the PSPF policy: Separating personnel).

11. **Table 1** describes the mandatory pre-employment screening checks outlined in **Requirements 1a and 1b**.

Table 1 Mandatory pre-employment screening checks

Screening check	Rationale
Identity check	An identity check helps to establish confidence in a person's identity and provides entities with a level of assurance about the prospective employee. The Attorney-General's Department recommends that the identity of all new personnel be verified to at least **Level of Assurance 3** of the National Identity Proofing Guidelines. **Level of Assurance 3** checks include: a. the uniqueness of the identity in the intended context b. the claimed identity is legitimate c. the operation of the identity in the community over time d. the linkage between the identity and the person claiming the identity e. the identity is not known to be used fraudulently. The core PSPF requirement for eligibility and suitability of personnel mandates that entities verify the person's identification documents with the issuing authority by using the Document Verification Service for Australian issued primary identification documents.
Eligibility to work in Australia	This check confirms whether a person is eligible to work in Australia. This requires confirming 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. Information on how to confirm Australian citizenship and verify visas is available on the Department of Home Affairs website.

12. **Table 2** details the recommended pre-employment checks that may assist entities to assess a person's suitability, in accordance with **Requirement 1c**. The Attorney-General's Department recommends that entities undertake pre-employment screening to Australian Standard AS 4811-Employment Screening.

Table 2 Recommended pre-employment screening checks

Screening check		Rationale
Integrity & reliability checks	Employment history check	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. The Attorney-General's Department recommends checking the employment history of all new personnel for a period of at least 5 years, where applicable.
	Residential history check	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. The Attorney-General's Department recommends checking residential history for all new personnel for a period of at least 5 years. It is recommended that entities make an assessment of whether the person's explanation about periods of residency for which they cannot provide supporting documents is reasonable.
	Referee checks	A referee check helps entities engage people of the appropriate quality, suitability and integrity. The Attorney-General's Department recommends conducting professional referee checks covering a period of at least the last 3 months. A referee check may address: a. any substantiated complaints about the person's behaviour b. information about any action, investigation or inquiry concerning the person's character, competence or conduct c. any security related factors that might reflect on the person's integrity and reliability.
	National police check	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. For information, 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	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. The Attorney-General's Department recommends checking a person's credit history. 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.
Qualification check		A qualification check verifies a person's qualifications with the issuing authority. The Attorney-General's Department recommends verifying declared academic qualifications with the issuing authorities, including universities, technical colleges or schools, as well as any professional associations or memberships that are required.

Screening check	Rationale
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 resources. A conflict can be brought by (and not limited to) financial particulars, secondary employment and associations. The Attorney-General's Department recommends that entities have a conflict-of-interest policy, that guides staff on what could be perceived as a conflict of interest and when and how to report a conflict. Based on their risk assessment, entities are encouraged to consider whether all personnel, not just contractors, complete a conflict-of-interest declaration. For advice, see the APSC publication Conflicts of interest.
Entity-specific checks	The Attorney-General's Department recommends entities identify 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. The Attorney-General's Department recommends entities seek separate advice from the Australian Public Service Commission, the Australian Human Rights Commission or independent legal advice about the suitability and use of any proposed entity-specific checks. 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.

C.1.1 Privacy and confidentiality

13. Pre-employment screening checks, including related security clearance vetting and ongoing suitability checks, are conducted in accordance with the Australian Privacy Principles. The Attorney-General's Department recommends obtaining 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. The Attorney-General's Department recommends entities 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:
    a. collect personal information, including sensitive information, from other entities or private organisations
    b. disclose personal information, including sensitive information, with other entities when determining initial or continuing suitability to access official resources
    c. use personal information, including sensitive information, to determine a person's ongoing suitability to access Australian Government resources
    d. transfer information to another entity when personnel transfer.
14. As part of the pre-employment screening, entities are also encouraged to obtain both:
    a. a statutory declaration stating all information provided is truthful and complete
    b. a signed agreement to confirm their undertaking to safeguard Australian Government resources including reference to compliance with relevant legislation and policies.
15. In addition to secrecy provisions under the Commonwealth *Criminal Code*, entities are encouraged to advise all personnel of any entity-specific legislative requirements.

C.1.1.1 Handling and managing personal information (including sensitive information)

16. When receiving and using this information sponsoring entities will need to consider its privacy obligations under the Australian Privacy Principles.
17. The Attorney-General's Department recommends entities establish robust procedures and practices to appropriately handle and manage this information. This includes 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 a vetting agency that has been identified through a vetting process (see **Requirements 3d**, **3e** and **3f**). These mechanisms can

support ongoing monitoring of security risk information. For further information see PSPF Policy: Ongoing assessment of personnel.

18. Due to the nature of its content, personal information will always be marked as at least Official: Sensitive. In limited circumstances, it may be necessary to apply a security classification. It is subject to the requirements for protecting the confidentiality, availability and integrity of information that are set out in PSPF Policy: Sensitive and classified information. This includes the secure transmission and storage of information.

C.2 Security clearances

C.2.1 Identify and record positions that require a security clearance

19. Personnel in certain positions may require a security clearance to access particular Australian Government resources (people, information and assets) relevant to their position. In accordance with an entity's physical and information security profile (see the PSPF policy: Security planning and risk management), this may include access to specific areas of an entity's facilities or specific ICT 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 integrity. This may be appropriate for positions where:
    a. the occupant will have access to aggregations of information or assets or
    b. the nature of the role requires greater assurance about the person's integrity, for example as a fraud mitigation or anti-corruption measure.
20. **Requirement 2** mandates that entities identify and record positions that require a security clearance and the level of clearance required. The Attorney-General's Department recommends that entities keep a register identifying:
    a. positions that require a security clearance for ongoing access to Australian Government resources
    b. positions that require a security clearance as a higher level assurance of personnel suitability
    c. when the requirement for a security clearance will be assessed (at least each time the position becomes vacant and before it is advertised).
21. The PSPF policy: Access to information provides information on the exemption from holding a security clearance for certain Australian public office holders accessing classified information. This exemption does not apply to staff of public office holders.
22. *Special Minister of State Determination 2018/27* provides that staff of ministers employed under Part III of the *Members of Parliament (Staff) Act 1984* obtain and maintain a Negative Vetting 2 security clearance. This determination permits variation in certain circumstances for electorate officers, see **Annex B**.

C.2.2 Eligibility for a security clearance

23. To be eligible for an Australian Government security clearance, an individual must be an Australian citizen and have a checkable background (see **Requirements 2**). A clearance subject has an uncheckable background when the vetting agency cannot complete the minimum checks and inquiries for the required period, or the checks and inquiries made do not provide adequate assurance about 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 vetting agency will deny the request for a clearance.
24. In accordance with **Requirements 2d** and **2e**, an accountable authority may waive the citizenship or checkable background requirements for a security clearance if there is an exceptional business requirement and after conducting a risk assessment.[1] Where an eligibility waiver has been issued, the vetting agency can still deny a security clearance if there are significant concerns about the clearance subject's eligibility or

[1] For locally engaged personnel, an entity may grant a waiver for citizenship eligibility where the preferred person is not an Australian citizen and the entity understands and agrees to manage that risk.

suitability to hold the clearance that cannot be mitigated (see **Requirement 3**). This includes concerns relating to the eligibility condition that was waived.

25. 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.

26. 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 under the PSPF policy: Reporting on security.

C.2.2.1 Exceptional business requirement

27. The Attorney-General's Department recommends that the accountable authority consider the following when establishing an exceptional business requirement:

    a. whether the role is critical to meeting the sponsoring entity's outcomes

    b. whether the role can be performed by a person who meets the eligibility requirements (ie is there another person capable of performing the role who is an Australian citizen and/or has a checkable background)

    c. whether the role can be redesigned, so that the access to classified information or resources is restricted to personnel who already hold or are eligible to hold the appropriate security clearance.

28. The Attorney-General's Department recommends that eligibility for a security clearance be included as a condition of employment in all recruitment actions relating to positions identified as requiring a security clearance.

C.2.2.2 Risk assessment

29. Entities must conduct security risk management in accordance with the PSPF policy: Role of accountable authority. When conducting a risk assessment for an eligibility waiver, the Attorney-General's Department recommends the accountable authority also consider the following:

    a. potential conflicts of interest

    b. advice from the authorised vetting agency and ASIO, including:

        i. for uncheckable backgrounds, details of the security concerns associated with the subject's uncheckable background and assessment of the impact of this uncheckable period against the whole-of-person assessment

        ii. for all waivers, any known concerns about the clearance subject

        iii. any threat assessments from ASIO on the clearance subject's country(ies) of citizenship or the country(ies) that give rise to issues of uncheckability

        iv. consultation with third parties whose resources (information, assets or personnel) may be accessed by the clearance subject and especially the originating or controlling entity of any TOP SECRET resources and any foreign entities

    c. for citizenship waivers:

        i. details of the clearance subject's visa status and whether they are actively seeking Australian citizenship, or plan to

        ii. the sponsoring entity's plan to ensure the clearance subject does not access caveated AUSTEO information

        iii. any threat assessments from ASIO on the clearance subject's country(ies) of citizenship or the country(ies) that give rise to issues of uncheckability

        iv. consultation with third parties whose resources (information, assets or personnel) may be accessed by the clearance subject, and especially the originating or controlling entity of any TOP SECRET resources and any foreign entities

d. the period covered by the waiver

e. proposed risk mitigations, including any conditions placed on the clearance holder subject to the waiver.

C.2.3 Recognising existing security clearances

30. Where an individual holds, or has previously held, a security clearance issued by an authorised vetting agency[2] at the level required for the identified position (or higher), an entity may assume sponsorship of that security clearance. The Attorney-General's Department recommends that prior to seeking a new security clearance, sponsoring entities identify whether the clearance subject already holds, or has previously held, a security clearance and advise the authorised vetting agency accordingly. The vetting agency will confirm the clearance details with the granting agency, obtain the clearance subject's personal security file and record the new sponsorship of the security clearance on the file.

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

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

i. for Baseline clearances, 15 years

ii. for Negative Vetting Level 1, 10 years

iii. for Negative Vetting Level 2, seven years

iv. for Positive Vetting, seven 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 two years; the SMSMP-PVG is available to entity security advisors or by request via the PSPF community on GovTEAMS)

b. the 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

c. the clearance was granted on the basis of an eligibility (citizenship or background) waiver

d. the clearance was granted subject to specific clearance maintenance requirements

e. the clearance has ceased.

32. If a clearance is subject to an eligibility waiver or specific clearance maintenance requirements, the vetting agency will advise the gaining sponsoring entity. For clearances subject to an eligibility waiver, the gaining sponsoring entity will accept and undertake the exceptional business requirement and risk assessment provisions in accordance with **Requirements 2d** and **2e**, prior to requesting transfer of sponsorship. For clearances subject to specific clearance maintenance requirements, the gaining sponsoring entity will need to accept the clearance conditions.

C.2.4 Clearance status

33. The definitions in **Table 3** describe the status of a security clearance.

Table 3 Security clearance status

Clearance status	Definition
Active	A maintained security clearance that is: a. sponsored by an Australian Government entity, and b. being maintained by a clearance holder and sponsoring entity.
Inactive	A security clearance that is within the revalidation period, however, the clearance is: a. not sponsored by an Australian Government entity, or b. not being maintained by the clearance holder for a period greater than six months due to long term absence from their role (eg maternity leave, extended leave without pay).

[2] 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.

Clearance status	Definition
	For Positive Vetting clearances, the SMSMP-PVG requires an annual security check to have been completed within the last two years.
Expired	A security clearance that is: a. outside the revalidation period, or b. a Positive Vetting clearance and an annual security check has not been completed within the last two years. It is not possible to request sponsorship of an expired clearance. If an Australian Government entity requests sponsorship after the end of the revalidation period, a new initial security clearance assessment process will be initiated.
Ceased	A security clearance (or in some circumstances vetting process): a. that has been denied or revoked, or b. that has time-based conditions on when the clearance subject or holder can reapply for a security clearance, or c. where the clearance subject or holder is ineligible to hold or maintain a security clearance.

C.3 Personnel security vetting standards

C.3.1 Authorised vetting agencies

34. The PSPF policy: Eligibility and suitability of personnel mandates that entities use AGSVA to conduct vetting, or where authorised, conduct security vetting in a manner consistent with the personnel security vetting standards.

35. Security vetting can be conducted by:

    a. AGSVA, which can 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

    b. an authorised vetting agency that can issue security clearances for its 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.

36. The personnel security vetting standards use the term 'assessing officer' to denote a person within an authorised vetting agency who conducts vetting assessments. The standards use the term 'security clearance delegate' to denote a person formally authorised to make decisions on the outcome of a vetting process (ie to grant, deny, grant-conditional or cancel a security clearance), see section C.3.5.

C.3.1.1 Issuing clearances

37. **Requirement 3a** mandates that vetting agencies only issue a security clearance where the clearance is sponsored by an Australian Government entity or otherwise authorised by the Australian Government. State and territory governments may request that AGSVA conduct security clearances for their personnel up to and including Negative Vetting 2, in accordance with the 2006 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.

38. Locally engaged personnel 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. The Department of Foreign Affairs and Trade is responsible for the security vetting of their locally engaged staff. The Australian Trade Commission is a managing entity under this directive and conducts security screening for its locally engaged staff and for those of attached entities.

C.3.2 Consent to share personal information

39. **Requirement 3b** mandates that vetting agencies 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. The Attorney-General's Department recommends that vetting agencies consider the guidance provided at C.1.1.

40. 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 policy: Ongoing assessment of personnel to share information of security concern, it is recommended that vetting agencies 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 vetting agencies. The Attorney-General's Department recommends that consent is obtained at key information collection points, such as application for a security clearance, and that consents are updated at reasonable intervals.

C.3.3 Personnel security adjudicative guidelines

41. **Requirement 3ci** mandates that vetting agencies assess an individual's eligibility and suitability to hold a security clearance by considering their integrity in accordance with the Personnel Security Adjudicative Guidelines (**Annex A**). For the purposes of security vetting, integrity is defined as the character traits of honesty, trustworthiness, maturity, tolerance, resilience and loyalty.

42. The Personnel Security Adjudicative Guidelines (at **Annex A**) provide the common risk factor areas against which a clearance subject's eligibility and suitability is assessed. These areas may have a bearing on one or more of a clearance subject's character traits. The Attorney-General's Department recommends vetting agencies use a process of structured professional judgement to achieve an overall determination based on the available information.

C.3.4 Minimum personnel security checks for a security clearance

43. **Requirement 3cii** mandates the minimum checks for a security clearance, these are outlined in **Table 4**. The effectiveness of these checks relies on complete, consistent and accurate information provided by the clearance subject. The Attorney-General's Department recommends that vetting agencies confirm:

    a. all documents requiring signature and witnessing have been signed and that signatures and dates of signatures match

    b. details provided by the clearance subject match supporting documents

    c. referees are appropriate and their contact details are provided

    d. financial statements (if applicable) are provided and complete.

Table 4 Minimum personnel security checks and requirements for a security clearance

<table>
<tr><th>Vetting check</th><th>Rationale</th></tr>
<tr><td>Confirmation of identity and verification of identity documents</td><td>Requirement 3cii mandates for all clearance levels (Baseline to Positive Vetting, inclusive) that vetting agencies confirm the identity of a clearance subject and verify identification documents. For Australian issued primary identification documents, authorised vetting agencies must verify the person's identification documents with the issuing authority by using the Document Verification Service.

The Attorney-General's Department recommends vetting agencies verify the identity of all clearance subjects in accordance with the National Identity Proofing Guidelines. Security vetting requires assurance of identity as follows:
<table>
<tr><th>Security clearance</th><th>Baseline Vetting</th><th>Negative Vetting 1</th><th>Negative Vetting 2</th><th>Positive Vetting</th></tr>
<tr><td>Assurance of identity</td><td colspan="2">High assurance to Level 3 of the National Identity Proofing Guidelines.</td><td colspan="2">Very high assurance to Level 4 of the National Identity Proofing Guidelines.</td></tr>
</table>
Levels of Assurance 3 and 4 constitute the following checks:
a. uniqueness of the identity in the intended context</td></tr>
</table>

Vetting check	Rationale
	b. the claimed identity is legitimate c. the operation of the identity in the community over time d. the linkage between the identity and the person claiming the identity e. the identity is not known to be used fraudulently f. only original physical documents shall be accepted (**Level 4**).
Confirmation of Australian citizenship and status of any other citizenships	**Requirement 3cii** mandates for all security clearance levels (Baseline to Positive Vetting, inclusive) that vetting agencies confirm the Australian citizenship of a clearance subject and assess whether they hold any other citizenships. 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, in accordance with **Requirement 2d**. Evidence of other citizenships or nationalities may have bearing on one or more of the risk factors, including external loyalties, influences and associations.

Background assessment

Requirement 3cii mandates for all clearance levels (Baseline to Positive Vetting, inclusive) that vetting agencies assess a clearance subject's background for the relevant checking period.

Security clearance	Baseline Vetting	Negative Vetting 1	Negative Vetting 2	Positive Vetting
Relevant checking period	5 years	10 years	10 years	Greater of 10 years or from the age of 16

The primary reason for examining an individual's background is to assess their integrity. The Attorney-General's Department recommends vetting agencies use a questionnaire to gather initial background assessment information from clearance subjects.

A vetting agency assesses a clearance subject as having an uncheckable background when the assessing officer cannot complete the required minimum checks and inquiries for the relevant period or the assessing officer does not have sufficient confidence in the quantity, quality, credibility or reliability of the information provided. For example, a background may be assessed as uncheckable because:

a. background assessment cannot be confidently conducted in certain countries of former residence
b. certain documents do not exist (they never existed or no longer exist) or it is not possible to get copies from the issuing authority
c. the source of the documents or information about the clearance subject may not be assessed as credible or reliable
d. there are significant gaps [Note i] 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. 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.

The primary reason for assessing whether a person has a checkable background is consideration of the security risk to the Australian Government, should that person be granted a security clearance.

If the vetting agency has exhausted all reasonable and available checking avenues and determined that a clearance subject's background is uncheckable, the vetting agency may:

a. 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 **Requirement 3d** and request an eligibility waiver from the sponsoring entity (see C.2.2)
b. if there are other concerns or identified risks that cannot be mitigated, advise the sponsoring entity that the clearance cannot be progressed.

Reasonable and available checking avenues in Australia or overseas include, but are not limited to, the following sources:

a. corroboration from a credible referee
b. government agencies and bodies
c. academic institutions
d. local police records, if available (obtained domestically through liaison with the AFP or internationally through the Department of Foreign Affairs and Trade)
e. humanitarian and aid agencies that maintain records for displaced persons
f. places of worship, for birth, death and marriage information in lieu of government records
g. private companies with whom the clearance subject has been employed
h. the Department of Home Affairs for records of all Australian entries and exits.

The Attorney-General's Department recommends that vetting agencies 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.

Separately, ASIO considers the background of clearance subjects as part of its security assessment. In some cases, ASIO will conclude an individual has an uncheckable background (eg because reliable

Vetting check	Rationale
	security checking cannot be undertaken for the relevant countries) and will communicate this via a security assessment.
Official secrets declaration check	**Requirement 3cii** mandates for all clearance levels (Baseline to Positive Vetting, inclusive) that vetting agencies obtain acknowledgement from the clearance subject of their responsibilities for the protection of official information. An official secrets declaration confirms that those accessing Australian Government resources understand their roles and responsibilities in relation to the protection of official information. This includes the consequences of the misuse or disclosure of official information and the application of criminal offences.
Statutory declaration	**Requirement 3cii** mandates for all clearance levels (Baseline to Positive Vetting, inclusive) that clearance subjects 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: a. copies of documents cannot reasonably or readily be obtained from the issuing authority within the required time b. a reasonable delay is expected and the clearance subject undertakes to provide the documents as soon as they are received. The Attorney-General's Department recommends that vetting agencies not accept a statutory declaration for: a. primary identification documents issued by an Australian authority b. proof of current employment c. proof of current residential address d. primary identification documents issued by a foreign authority where it is possible to obtain these documents e. corroboration of gaps identified in determining a clearance subject's checkable background. For information about statutory declarations, see the Attorney-General's Department website.

Referee checks

Requirement 3cii mandates for all clearance levels (Baseline to Positive Vetting, inclusive) that vetting agencies obtain referee reports about a clearance subject's eligibility and suitability to hold a security clearance as follows:

Security clearance	Baseline Vetting	Negative Vetting 1	Negative Vetting 2	Positive Vetting
Referee check*	At least one professional referee	At least one professional referee, and one personal referee	At least one professional referee, one personal referee, and one un-nominated referee	At least one professional referee, one personal or peer referee, and one un-nominated referee

*Referees should collectively cover the whole checkable period for all levels of security clearance.

Professional referees to cover a period of at least the preceding 3 months.
Personal referees to 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 months.

Personal and professional 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:

a. current and previous address
b. current and previous employment
c. overseas travel
d. financial status
e. use of alcohol and drugs.

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.

The Attorney-General's Department recommends that vetting agencies contact previous government employers to determine if the person 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.

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 resources may be questionable.

Do 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.

There are benefits to conducting at least one face-to-face referee interview. For example, 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.
For further information on conducting referee checks for Positive Vetting security clearances see the SMSMP-PVG.

Digital footprint check

Requirement 3cii mandates for all clearance levels (Baseline to Positive Vetting, inclusive) that vetting agencies 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 check is the unique pattern of electronic transactions made by an individual's publicly accessible online presence. An assessment of an individual's digital footprint can provide insight into their life, interactions and personal views. This information may identify behaviours of security concern, or provide further assurance that a clearance subject has provided a full and truthful account of information relevant to the assessment of their integrity.

The Attorney-General's Department recommends that vetting agencies refer to the digital footprint check framework (**Annex E**) when establishing procedures for conducting these checks.

National police check

Requirement 3cii mandates for all clearance levels (Baseline to Positive Vetting, inclusive) that vetting agencies obtain a national police check for the clearance subject.

A national police check is carried out by the 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. For information, see the OAIC – Spent Conviction Scheme Fact Sheet.

The application of the Spent Conviction Scheme for relevant clearance levels is as follows:

Security clearance	Baseline Vetting	Negative Vetting 1	Negative Vetting 2	Positive Vetting
Application of the Spent Conviction Scheme	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: a. it has been 10 years from the date of the conviction (or five years for juvenile offenders) b. the individual was not sentenced to imprisonment for more than 30 months c. the individual has not re-offended during the 10 year (five years for juvenile offenders) waiting period and d. a statutory or regulatory exclusion does not apply.	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.		

For information, see the National Police Check pages on the AFP website.

Financial history assessment	**Requirement 3cii** mandates for all clearance levels (Baseline to Positive Vetting, inclusive) that vetting agencies conduct a financial history assessment. The purpose of this assessment is to consider whether: a. the clearance subject is living beyond their means, for example spending more than they earn or is impulsive and irresponsible with their spending b. there is any history of unmanaged debt c. the clearance subject has failed to meet financial obligations, including submission of tax returns, payment of rent and debts, bankruptcy and denial of credit. Where there are concerns about a clearance subject's financial situation, particularly unexplained wealth or a high level of debt, additional checks may be warranted. The Attorney-General's Department recommends that vetting agencies determine appropriate checks on a case-by-case basis. Where a clearance subject has indicated that they have been bankrupt or insolvent, the Attorney-General's Department recommends that the vetting agency request a bankruptcy check in writing through the Insolvency and Trustee Service Australia. 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, the vetting agency may seek a credit history check from an accredited financial credit check organisation.
Financial statement	**Requirement 3cii** mandates for Negative Vetting 1 and above clearance levels that vetting agencies require clearance subjects to complete a financial statement. 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. The Attorney-General's Department recommends that assessing officers undertake specialist training or seek specialist advice before undertaking complex financial analysis.
ASIO security assessment	**Requirement 3cii** mandates for Negative Vetting 1 and above clearance levels (or lower levels where concerns have been identified) that vetting agencies obtain an ASIO security assessment. Part IV of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) provides for ASIO to undertake security assessments of people. For the purposes of security clearances, the ASIO security assessment provides a recommendation to the vetting agency on the security suitability of the clearance subject to access any information or place, access to which is controlled or limited on security grounds, and may provide additional advice including advice on conditions that might be placed on a clearance. That recommendation is based on an assessment of the risk to security (as defined in the ASIO Act) that would be associated with granting a clearance to the subject. 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 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. Vetting agencies request the ASIO security assessment after all other checks and the clearance interview (if required, see below) are complete. This prevents unnecessary use of ASIO resources where the clearance subject would not otherwise be recommended for a clearance. The Attorney-General's Department recommends that vetting agencies negotiate with ASIO on a case-by-case basis where operational needs require the ASIO security assessment to be conducted concurrently with other checks.

Security interview

Requirement 3cii mandates that vetting agencies conduct interviews of clearance subjects as follows:

Security clearance	Baseline Vetting	Negative Vetting 1	Negative Vetting 2	Positive Vetting
Interviews of clearance subjects for the relevant checking period	Interview not required unless: a. the citizenship or background check requirements have been waived b. there are particular suitability concerns about a clearance subject.		Face-to-face (video or telephone in exceptional circumstances) interview addressing: a. external loyalties, influences and associations b. personal relationships and conduct c. financial considerations d. alcohol and drug use e. criminal history and conduct f. security attitudes and violations g. emotional and mental health issues.	

The Attorney-General's Department recommends that face-to-face (wherever possible), and video or telephone interviews (where circumstances necessitate), address all factor areas in the Personnel Security Adjudicative Guidelines, and any specific areas of concern.

The Attorney-General's Department recommends that supplementary interviews be conducted for all clearance levels where specific areas of concern arising from internal and external checking have not been adequately resolved by other supplementary checks. It is recommended that supplementary interviews address the specific areas of concern. If any further concerns are identified at the interview, it is recommended that supplementary interviews be conducted face-to-face wherever possible for significant or complex issues. However, a telephone interview may be conducted to resolve minor issues or where a face-to-face interview is not possible (eg the clearance subject is travelling overseas).

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.

For further information on conducting security interviews for Positive Vetting security clearances see the SMSMP-PVG.

Psychological assessment

Requirement 3cii mandates that vetting agencies 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.
For further information on conducting psychological assessments see the SMSMP-PVG.

Financial probity assessment

Requirement 3cii mandates for Positive Vetting clearance levels that vetting agencies undertake a probity assessment into a clearance subject's financial circumstances.

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.

For further information on conducting financial probity assessments, see the SMSMP-PVG.

Table 4 notes:

[i] A significant gap is considered to be greater than 12 months (cumulative) out of Australia within the background assessment period.

44. Vetting agencies may conduct additional vetting checks or assessments where they have access to additional capabilities, such as criminal intelligence checks, 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 5** provides two examples of additional vetting checks that may be undertaken for security clearances.

45. While not mandated for Baseline, Negative Vetting 1 and Negative Vetting 2 clearances, the Attorney-General's Department recommends that vetting agencies seek advice from a duly qualified mental health practitioner where the vetting agency identifies a mental health condition that may affect the clearance subject's ability to protect Australian Government resources.

Table 5 Example additional checks for security clearances

Vetting check	Rationale
Criminal intelligence check	The Attorney-General's Department recommends that vetting agencies with available criminal intelligence capabilities conduct a 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	The Attorney-General's Department recommends mental health assessments only occur where the vetting agency identifies issues related to the clearance subject's ability to protect Australian Government resources. Having a mental health condition does not necessarily mean that a clearance subject would not be able to protect Australian Government resources. The Attorney-General's Department recommends that where the vetting agency is concerned that the clearance subject's emotional stability or psychological health may affect their ability to protect Australian Government resources, the 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 a 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.

C.3.5 Outcomes of security vetting process

46. 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:

    a. against the Personnel Security Adjudicative Guidelines (**Annex A**)

    b. taking into account all relevant, reliable and independently verified information obtained through the minimum personnel security checks, and any additional checks required

    c. resolving any doubt in the national interest, in accordance with **Requirement 3ciii**.

47. The Attorney-General's Department recommends that an assessing officer conduct the assessment and provide a security clearance delegate with a recommended outcome (see **Table 6**). Information to support the assessment includes:

    a. any gaps in the checkable period where supporting documents were not available, how these gaps were mitigated and if supplementary checks were undertaken to this effect

    b. any anomalies or issues identified, how these anomalies and issues were mitigated and if supplementary checks were undertaken

    c. any eligibility waivers provided by the sponsoring entity.

48. In determining the security clearance outcome based on the recommendation from the assessing officer, the delegate:
    a. satisfies themselves that all issues raised in the clearance process have been addressed
    b. provides the clearance subject with the opportunity to respond to any adverse information, if appropriate.

Table 6 Determinative outcomes of the security vetting process

Outcome	Description
Denied	The clearance subject is not suitable to hold an Australian Government security clearance at the requested level.
Granted	The clearance subject is eligible and suitable to hold an Australian Government security clearance.
Granted–conditional	The clearance subject is eligible and suitable to hold an Australian Government security clearance if they comply with conditions and/or specific clearance maintenance requirements.

49. The Attorney-General's Department recommends that vetting agencies use consistent language to describe the outcomes of security vetting processes in personal security files. **Table 7** provides labels and descriptions for possible administrative outcomes of the security vetting process. These apply where no vetting assessment or determination has been made.

Table 7 Administrative outcomes of the security vetting process

Outcome	Description
Ineligible	The clearance subject is not eligible for an Australian Government security clearance as they: a. do not hold Australian citizenship b. do not have a checkable background.
Cancelled	The security clearance could not be completed by the vetting agency because: a. sponsorship of the clearance was removed at the request of the sponsoring entity b. sponsorship or clearance requirement could not be confirmed c. the clearance subject was non-compliant.

50. The Attorney-General's Department recommends that the vetting agency provides a summary of information when notifying the clearance subject and sponsoring entity of the security clearance outcome. This includes:
    a. the level of clearance the subject is being assessed against
    b. the date of the determination of ineligible, granted, granted–conditional, denied or cancelled
    c. any eligibility (background or citizenship) waiver granted in the clearance process and any conditions placed by virtue of the waiver
    d. any conditions required as part of a granted–conditional clearance
    e. the date for revalidation
    f. details of the review and appeals processes open to the clearance subject, if applicable.
51. In addition, **Requirements 3d, 3e** and **3f** mandate that vetting agencies provide relevant information of security concern obtained during the security vetting process to the sponsoring entity. This is particularly important if identified security concerns may lead to an adverse recommendation. In these circumstances the vetting agency (where a determination is still pending, including circumstances where a response has been invited from the clearance subject in relation to the identified risks) shares only relevant information with the sponsoring entity to enable temporary mitigations until a final outcome is made.
52. **Requirement 3g** mandates that vetting agencies apply the rules of procedural fairness, without compromising the national interest, when making security clearance assessments and determining a security clearance outcome. See section C.3.6 for further information.

C.3.5.1 Conditional security clearances

53. **Requirement 3e** mandates that if information of security concern is identified during the vetting process that is not sufficient to deny a clearance and the related risks can be managed through conditions attached

to the security clearance, the vetting agency is to provide the sponsoring entity with information to inform a risk assessment. Before issuing the security clearance the sponsoring entity's accountable authority (or Chief Security Officer) and the clearance subject need to agree to any conditions associated with the clearance.

54. Security clearance conditions enable the sponsoring entity to manage ongoing risks affecting the clearance subject's eligibility and suitability to hold a security clearance. This may include access restrictions or other risk mitigation measures. Monitoring a clearance subject's compliance with security clearance conditions is a supporting requirement of the PSPF policy: Ongoing assessment of personnel. Non-compliance with conditions may trigger a review for cause.

C.3.5.2 Sharing other relevant information of security concern

55. **Requirement 3f** mandates that vetting agencies advise the sponsoring entity of any other relevant information of security concern identified during the vetting process when advising the sponsoring entity of the security clearance outcome. This may include (but is not limited to) information relating to any vulnerabilities or risk factors and risk mitigation measures that were applied by the vetting agency. The sponsoring entity can then understand and manage any risks relating to the clearance holder's ongoing access to Australian Government resources. For information, see the PSPF policy: Ongoing assessment of personnel.

C.3.6 Procedural fairness

56. **Requirement 3g** mandates that vetting agencies apply procedural fairness to security clearance determinations that are adverse to a clearance subject, without compromising the national interest or betraying the confidentiality of the source. 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.

57. If the assessing officer intends to recommend against the approval of a clearance at the level sought, or to recommend that the clearance be approved with specific clearance maintenance requirements, the Attorney-General's Department recommends that the clearance subject 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.

58. The Attorney-General's Department recommends that vetting agencies provide the clearance subject with a written statement identifying any concerns. It is recommended that 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.

59. The Attorney-General's Department recommends that vetting agencies consider whether an outsourced vetting service provider is able to manage procedural fairness issues involving outsourced vetting services.

60. For details, refer to **Annex C** and **Annex D**.

C.3.7 Competencies of vetting personnel

61. **Requirement 3h** mandates that authorised vetting agencies ensure vetting personnel (ie assessing officers and security clearance delegates) have and maintain the required skills and competencies for their role.

62. The Attorney-General's Department recommends that vetting personnel be able to demonstrate competencies and skills that include:

    a. knowledge of and the ability to conduct personnel security assessments

    b. understanding of the security vetting process and the PSPF

    c. knowledge of the security environment and ability to use ASIO intelligence

    d. knowledge of and the ability to apply relevant public sector legislation, including espionage offences and the *Privacy Act 1988*

    e. knowledge of and the ability to apply the principles of natural justice and procedural fairness

f. general skills and competencies, including:
    i. handling official information
    ii. workplace communications
    iii. relevant interviewing skills
    iv. data analysis
    v. administration, including records management.

63. The Attorney-General's Department notes that the above competencies and skills can be attained through formal qualifications, such as the Certificate IV or Diploma in Government Security, or equivalent qualifications. Where vetting agencies determine that a formal qualification is required for vetting personnel in the agency, the Attorney-General's Department recommends that qualifications be obtained from a registered training organisation. A list of registered training organisations is available at www.training.gov.au.

D. Find out more

64. Further information on employment and entity-specific screening can be found in the Australian Standards publications:

a. AS4811-2006: Employment Screening
b. HB 323-2007: Employment Screening Handbook
c. AS 8001-2008: Fraud and Corruption Control.

D.1 Change log

Table 8 Amendments in this policy

Version	Date	Section	Amendment
v2018.0	Sep 2018	Throughout	Not applicable. This is the first issue of this policy
v2020.1	Mar 2020	Throughout	Updated hyperlinks; changed references to GovDex to GovTEAMS.
V2020.2	Aug 2020	Throughout	Changes to policy aims to provide clarification and correction, and to align it with the Personnel Security Risk Information Sharing Framework, in particular language around conditional clearances.

Annex A. Personnel security adjudicative guidelines

Purpose

1. The Personnel Security Adjudicative Guidelines support vetting agencies in their assessment of a person's suitability to hold a security clearance, by assessing the individual against common risk factor areas. The guidelines apply to assessments of initial and ongoing suitability to access Australian Government resources.

Suitability to hold a security clearance

2. A clearance subject is suitable to hold a security clearance at any level where it is established, to the appropriate degree of satisfaction, that the clearance subject possesses and demonstrates an appropriate level of integrity (soundness of character and moral principle). 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. These character traits are:
    a. **honesty** – truthful and frank and does not have a history of unlawful behaviour
    b. **trustworthiness** – responsibility, reliability and maturity
    c. **maturity** – capable of honest self-appraisal and able to cope with stress; age is not necessarily a good indicator of maturity
    d. **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
    e. **resilience** – ability to adapt well in the face of adversity, trauma, tragedy, threats or significant sources of stress
    f. **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).
3. 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.
4. 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.
5. Each clearance subject is assessed on their own merits, and the final determination of their suitability rests with the authorised vetting agency delegate. Any doubt concerning the clearance subject's suitability must be resolved in favour of the national interest (see **Requirement 3c**).

Determining suitability

6. The determination of whether an individual is suitable to hold a security clearance, consistent with the national interest, is based on careful consideration of the whole person in the context of the following risk factor areas:
    a. external loyalties, influences and associations
    b. personal relationships and conduct
    c. financial considerations
    d. alcohol and drug usage

e. criminal history and conduct

f. security attitudes and violations

g. mental health disorders.

7. These factor areas may have a bearing on one or more of a clearance subject's character traits.

8. The Attorney-General's Department recommends vetting agencies use a process of structured professional judgement to come to an overall determination based on the available information.

Adverse information

9. Although adverse information concerning a single criterion may not be sufficient for an unfavourable determination, the clearance subject may be found unsuitable to hold the requested level of security clearance if available information reflects a current or recurring pattern of:

a. questionable judgement

b. dishonesty

c. intolerance/inflexibility

d. immaturity

e. untrustworthiness

f. irresponsibility

g. vulnerability to influence or coercion

h. emotionally unstable behaviour.

10. Reliable and significant adverse information may lead the security clearance delegate to deny or revoke the security clearance.

11. The Attorney-General's Department recommends that in evaluating the relevance of any conduct, the assessing officer and security clearance delegate consider the:

a. nature, extent and seriousness of the conduct

b. circumstances surrounding the conduct, including the degree of willing or knowledgeable participation

c. frequency and currency of the conduct

d. clearance subject's age and maturity at the time of the conduct

e. presence or absence of rehabilitation and other pertinent behavioural changes

f. motivation for the conduct

g. potential for pressure, coercion, exploitation or duress

h. likelihood of continuation or recurrence.

12. Vetting agencies must share relevant information of security concern about security clearance holders with sponsoring entities (see **Requirements 3e and 3f** of the PSPF policy: Eligibility and suitability and **Requirement 1bii** of the PSPF policy: Ongoing assessment of personnel). Adverse information about a clearance subject may not be sufficient for an unfavourable determination but may be relevant to a sponsoring entity's assessment of personnel security risk.

13. For security cleared personnel, sponsoring entities are responsible for assessing how information relates to the entity's security risk and 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 suitability to hold a clearance. The PSPF policy: Ongoing assessment of personnel core requirement 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 vetting agencies so that they can determine whether it is relevant.

14. The Attorney-General's Department recommends vetting agencies have 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.

Concerns about existing clearance holders

15. 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 assessing officer and the delegate considers whether the person:
    a. voluntarily reported the information
    b. responded to questions truthfully and completely
    c. sought assistance and followed professional guidance, where appropriate
    d. resolved or appears likely to favourably resolve the security concern
    e. has demonstrated positive changes in behaviour and employment.
16. If after evaluating material of security concern the delegate decides that the material is not serious enough to warrant a determination to revoke or downgrade the security clearance, the Attorney-General's Department recommends the vetting agency 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.

Risk factor areas

17. There are seven risk factor areas:
    a. external loyalties, influences and associations
    b. personal relationships and conduct
    c. financial considerations
    d. alcohol and drug use
    e. criminal history and conduct
    f. security violations
    g. emotional and mental health issues.

External loyalties, influences and associations

Concerns

18. All people working 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. However, the issue is whether a clearance subject recognises their responsibilities to their employing entity, the elected government and the public interest.
19. 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.
20. Involvement in certain types of outside employment or activities is of security concern if it poses a conflict with a clearance subject's security responsibilities and could create an increased risk of unauthorised disclosure of security classified information.

21. A security risk may exist when a clearance subject or their immediate family (including cohabitants and other persons to whom they may be bound by affection, influence or obligation) are not Australian citizens or may be subject to duress. These situations could potentially introduce foreign influence that could result in the compromise of security classified information. Contacts with citizens of other countries or financial interests in other countries are relevant to security determinations if they make the clearance subject potentially vulnerable to coercion, exploitation or pressure.

Conditions that could raise a security concern and may be disqualifying

22. Conditions that could raise a security concern and may be disqualifying include:

    a. Involvement in, support of, training to commit or advocacy of any act of:

        i. espionage
        ii. foreign interference
        iii. sabotage
        iv. urging violence
        v. terrorism
        vi. treason
        vii. politically motivated violence
        viii. communal violence
        ix. attacks on Australia's defence system
        x. serious threats to Australia's territorial or border integrity.

    b. Association or sympathy with persons who are attempting to commit, or who are committing, any of these above acts.

    c. Association or sympathy with persons or organisations that advocate, threaten, or use force or violence, or use any other illegal or unconstitutional means, in an effort to:

        i. overthrow or influence the Australian Government or any state or local government
        ii. prevent federal, state or local government personnel from performing official duties
        iii. gain retribution for perceived wrongs caused by the federal, state, or local government
        iv. prevent others from exercising their rights under the Constitution or laws of Australia or of any state or territory.

    d. Contact with a family member, business or professional associate, friend or other person who is a citizen of, or resident in, a foreign country, where that contact creates an unacceptably heightened risk of foreign exploitation, inducement, manipulation, pressure or coercion.

    e. Connections to a foreign person, group, government or country that creates potential conflict of interest between the clearance subject's obligation to protect Australian Government resources and their desire to help a foreign person, group or country by providing that information.

    f. Sharing living quarters with a person or persons, regardless of citizenship status, if that relationship creates a heightened risk of foreign or criminal inducement, manipulation, pressure or coercion.

    g. A substantial business, financial or property interest in a foreign country, or in any foreign-owned or foreign-operated business that could put the clearance subject at heightened risk of foreign influence or exploitation.

    h. Failure to report, when required, an association with a foreign national.

    i. Unauthorised association with a suspected or known agent, associate or employee of a foreign intelligence service.

j. Indications that representatives or nationals from a foreign country are acting to increase the vulnerability of the clearance subject to possible future exploitation, inducement, manipulation, pressure or coercion.

k. Conduct, especially while travelling outside Australia, which may make the clearance subject vulnerable to exploitation, pressure or coercion by a foreign person, group or government.

l. Exercise of any right, privilege or obligation of foreign citizenship after becoming an Australian citizen. This includes but is not limited to:

    i. possession of a current foreign passport

    ii. military service or a willingness to bear arms for a foreign country

    iii. accepting educational, medical, retirement, social welfare or other such benefits from a foreign country

    iv. residence in a foreign country to meet citizenship requirements

    v. using foreign citizenship to protect financial or business interests in another country

    vi. seeking or holding political office in a foreign country

    vii. voting in a foreign election.

m. Action to acquire or obtain recognition of a foreign citizenship by an Australian citizen.

n. Performing or attempting to perform duties or act to serve the interests of a foreign person, group, organisation or government in conflict with Australia's national interest.

o. Any statement or action that shows allegiance to a country other than Australia, for example, declaration of intent to renounce Australian citizenship or the renunciation of Australian citizenship.

p. Any employment or service, whether compensated or voluntary, with:

    i. the government of a foreign country

    ii. any foreign national, organisation or other entity

    iii. a representative of any foreign interest

    iv. any foreign, domestic, or international organisation, including media or a person engaged in analysis, discussion or publication of material on intelligence, defence, foreign affairs, protected technology or protective security

    v. failure to report or fully disclose an outside activity when this is required.

q. Ongoing voluntary association with individuals or groups of an extremist nature, for example, those who espouse beliefs incompatible with a liberal democracy.

Conditions that could mitigate security concerns

23. Conditions that could mitigate security concerns include:

a. The clearance subject was unaware of the unlawful aims of an individual or organisation and severed ties upon learning of these.

b. The clearance subject's involvement was only with the lawful or humanitarian aspects of an organisation.

c. Involvement in activities of concern occurred for only a short period of time and was attributable to curiosity or academic interest.

d. The involvement or association with the activities of concern occurred under such unusual circumstances, or so much time has elapsed, that it is unlikely to recur and does not cast doubt on the clearance subject's current reliability, trustworthiness or loyalty.

e. The nature of the relationships with foreign persons, the country in which these persons are located or the positions or activities of those persons in that country are such that it is unlikely the clearance

subject will be placed in a position of having to choose between the interests of a foreign individual, group, organisation or government and Australia's national interest.

f. There is no conflict of interest, either because the clearance subject's sense of loyalty or obligation to the foreign person, group, government or country is so minimal, or the clearance subject has such deep and longstanding relationships and loyalties in Australia that they can be expected to resolve any conflict of interest in favour of Australia's national interest.

g. Contact or communication with foreign citizens is casual and infrequent and there is little likelihood that it could create a risk for foreign influence or exploitation.

h. The foreign contacts and activities are on Australian Government business or are approved by the Chief Security Officer or delegate.

i. The clearance subject has promptly complied with requirements to report contacts, requests or threats from people, groups or organisations from a foreign country.

j. The value or routine nature of the foreign business, financial or property interests is such that they are unlikely to result in a conflict and could not be used to influence, manipulate or pressure the clearance subject.

k. Where reasons for possession or acquisition of multiple citizenship are not a security concern, including:

   i. multiple citizenship when based solely on a parent's citizenship or birth in a foreign country

   ii. marriage

   iii. convenience of travel.

l. The clearance subject has expressed a willingness to renounce other citizenships.

m. Exercise of the rights, privileges or obligations of foreign citizenship occurred before the clearance subject became an Australian citizen or when the clearance subject was a minor.

n. The use of a foreign passport is approved by the Chief Security Officer or delegate.

o. The foreign passport has been destroyed, surrendered or invalidated.

p. The vote in a foreign election was encouraged by the Australian Government.

Personal relationships and conduct

Concerns

24. Conduct involving questionable judgement, dishonesty or unwillingness to comply with rules and regulations can raise questions about the clearance subject's reliability, trustworthiness and ability to protect Australian Government resources.

25. Of special interest is any failure to provide truthful and candid answers during the security clearance process or a failure to cooperate with the security clearance process. Either of the following will normally result in denial or revocation of a security clearance, or administrative termination of further processing for a security clearance assessment:

   a. refusal or failure without reasonable cause to undergo or cooperate with the security clearance process, including meeting with an assessing officer for a security interview, completing security and consent forms and cooperation with supplementary evaluations and periodic reviews

   b. refusal to provide full, frank and truthful answers to relevant questions of assessing officers, or other official representatives in connection with a personnel security determination.

26. Sexual behaviour that involves a criminal offence indicates a personality or emotional disorder and reflects a gross lack of judgement and discretion. This may put the clearance subject in a position of undue influence or coercion, exploitation or duress that can raise questions about the clearance subject's reliability, trustworthiness and maturity. Sexual orientation is not relevant to these considerations.

Conditions that could raise a security concern and may be disqualifying

27. Conditions that could raise a security concern and may be disqualifying include:

    a. Deliberate omission, concealment or falsification of relevant facts from a personnel security questionnaire, personal history statement or similar form used to determine security clearance suitability, or providing misleading information to assessing officers or other officers involved in the clearance process.

    b. Credible adverse information in several adjudicative issue areas that is not sufficient for an adverse determination under any other single guideline, but when considered in total, supports a whole-of-person assessment of questionable judgement, untrustworthiness, unreliability, lack of candour, unwillingness to comply with rules and regulations or other characteristics indicating that the person may not properly safeguard official information.

    c. Credible adverse information that is not explicitly covered under any other guideline and may not be sufficient by itself for an adverse determination, but, when combined with all available information, supports a whole-of-person assessment of questionable loyalty, trustworthiness, honesty, maturity, tolerance or vulnerability to coercion or influence. This includes consideration of:

        i. untrustworthy or unreliable behaviour including breaches of client confidentiality, release of proprietary information, unauthorised release of sensitive corporate or other official government information

        ii. disruptive, violent or inappropriate behaviour in the workplace

        iii. a pattern of dishonesty or rule violations

        iv. evidence of significant misuse of government or other employer's time or resources.

    d. Sexual behaviour of a criminal nature, whether or not the clearance subject has been prosecuted.

    e. A pattern of compulsive, self-destructive or high-risk sexual behaviour that the person is unable to stop or that may be symptomatic of a personality disorder.

    f. Sexual behaviour that causes the clearance subject to be vulnerable to coercion, exploitation or duress.

    g. Personal conduct, or concealment of information about conduct, that creates a vulnerability to exploitation, manipulation or duress, such as:

        i. engaging in activities which, if known, may affect the person's personal, professional or community standing

        ii. while in another country, engaging in any activity that is illegal in that country or that is legal in that country but illegal in Australia and may serve as a basis for exploitation or pressure by the foreign security or intelligence service or other group.

    h. Violation of a written or recorded commitment made by the clearance subject to the employer as a condition of employment.

    i. Association with persons involved in criminal activity.

Conditions that could mitigate security concerns

28. Conditions that could mitigate security concerns include:

    a. The behaviour occurred prior to or during adolescence and there is no evidence of subsequent conduct of a similar nature.

    b. The behaviour no longer serves as a basis for coercion, exploitation or influence.

    c. The clearance subject made prompt, good faith efforts to correct the omission, concealment or falsification before being confronted with the facts.

    d. The refusal or failure to cooperate, omission or concealment was caused by or associated with improper or inadequate advice of government officers or legal counsel. Upon being made aware of

the requirement to cooperate or provide the information, the clearance subject cooperated fully and truthfully.

e. The behaviour or offence is so minor, or so much time has passed, or the behaviour is so infrequent, or it happened under such unique circumstances that it is unlikely to recur and does not cast doubt on the clearance subject's current reliability, trustworthiness or good judgement.

f. The clearance subject has acknowledged the behaviour and obtained counselling to change the behaviour or has taken other positive steps to alleviate the stressors, circumstances, or factors that caused untrustworthy, unreliable or other inappropriate behaviour. There is evidence that this treatment has been effective and such behaviour is unlikely to recur.

g. The clearance subject has taken positive steps to reduce or eliminate vulnerability to exploitation, manipulation or duress.

h. The information was unsubstantiated or from a source of questionable reliability.

i. Association with persons involved in criminal activity has ceased or occurs under circumstances that do not cast doubt upon the clearance subject's reliability, trustworthiness, judgement or willingness to comply with rules and regulations.

Financial considerations

Concerns

29. Failure or inability to live within one's means, satisfy debts or meet financial obligations may indicate poor self-control, lack of judgement or unwillingness to abide by rules and regulations. This may raise questions about a clearance subject's honesty, trustworthiness, maturity and vulnerability to coercion or influence.

30. A clearance subject who is financially overextended may be at a heightened risk of engaging in illegal acts including espionage to generate funds. This risk is further heightened if the financial difficulties have arisen from compulsive behaviour, for example gambling.

31. Unwillingness to pay debts where means are available may indicate untrustworthiness or lack of conscience regarding obligations.

32. Affluence that cannot be explained by known sources of income is a concern as it may indicate proceeds from financially profitable criminal acts.

Conditions that could raise a security concern and may be disqualifying

33. Conditions that could raise a security concern and may be disqualifying include:

a. Inability or unwillingness to satisfy debts.

b. Indebtedness caused by frivolous or irresponsible spending and the absence of any evidence of willingness or intent to pay the debt or establish a realistic plan to pay the debt.

c. A history of not meeting financial obligations.

d. Deceptive or illegal financial practices such as embezzlement, theft, fraud, tax evasion or other intentional breaches of trust.

e. Consistent spending beyond one's means, which may be indicated by excessive indebtedness, significant negative cash flow, high debt-to-income ratio or other financial analysis.

f. Financial problems that are linked to drug abuse, alcoholism, gambling addiction or other matters indicating compulsive behaviour or emotional or psychological instability that may have implications for the clearance subject’s maturity, trustworthiness and vulnerability to coercion or influence (refer to factor areas alcohol and drug usage, and emotional and mental health issues).

g. Repeated failure to meet Australian taxation requirements.

h. Unexplained affluence, as shown by a lifestyle or standard of living, increase in net worth, or money transfers that cannot be explained by the subject's known legal sources of income.

i. Compulsive or addictive gambling as indicated by an unsuccessful attempt to stop gambling, 'chasing losses' (ie increasing the bets or returning another day in an effort to get even), concealment of gambling losses, borrowing money to fund gambling or pay gambling debts, family conflict or other problems caused by gambling.

Conditions that could mitigate security concerns

34. Conditions that could mitigate security concerns include:

a. The behaviour happened so long ago, was so infrequent, or occurred under such circumstances that it is unlikely to recur and does not cast doubt on the clearance subject's current reliability, trustworthiness or good judgement.

b. The conditions that resulted in the financial problem were largely beyond the person's control (eg loss of employment, a business downturn, unexpected medical emergency or a death, divorce or separation) and the clearance subject acted responsibly.

c. The person has received or is receiving counselling for the problem or there are clear indications that the problem is being resolved or is under control.

d. The clearance subject initiated good faith efforts to repay overdue creditors or otherwise resolve debts.

e. The clearance subject has a reasonable basis to dispute the legitimacy of the debt and provides evidence of actions to resolve the issue.

f. The affluence resulted from a legal source of income.

Alcohol and drug use

Concerns

35. Excessive alcohol consumption often leads to questionable judgement or the failure to control impulses and can raise questions about a clearance subject's reliability, trustworthiness and ability to maintain discretion.

36. Drugs are mood and behaviour altering substances. They include drugs, materials and other chemical compounds identified and listed in Schedule 4 of the Customs (Prohibited Imports) Regulations 1956 and inhalants and other similar substances.

37. Drug abuse is the use of an illegal drug, or use of a legal drug in a manner that deviates from approved medical direction.

38. Use of illegal drugs or misuse of prescription drugs can raise questions about a clearance subject's trustworthiness and honesty because it may impair judgement and a person's ability or willingness to comply with laws, rules and regulations is questioned. Use of illegal drugs or misuse of prescription drugs may make the clearance subject vulnerable to coercion or influence.

Conditions that could raise a security concern and may be disqualifying

39. Conditions that could raise a security concern and may be disqualifying include:

a. Alcohol-related incidents away from work, such as driving while under the influence, fighting, child or spouse abuse, disturbing the peace or other incidents of concern, regardless of whether the clearance subject has been diagnosed as an alcohol abuser or is alcohol dependent.

b. Alcohol-related incidents at work, such as reporting for duty in an intoxicated or impaired condition, or excessive drinking while at work.

c. Habitual or binge consumption of alcohol to the point of impaired judgement.

d. Diagnosis by a duly qualified medical professional (eg physician, clinical psychologist, or psychiatrist) of alcohol or drug abuse or dependence.

e. Identification of alcohol or drug abuse or dependence by an accredited clinical social worker who is a staff member of a recognised alcohol or drug treatment program.

f. Relapse after diagnosis of alcohol or drug abuse or dependence and completion of an alcohol or drug rehabilitation program.

g. Criminal charges relating to alcohol or drug abuse or possession.

h. Failure to follow court orders regarding alcohol or drug education, evaluation, treatment or abstinence.

i. Any drug abuse.

j. Testing positive for illegal drug use.

k. Illegal drug possession, including cultivation, processing, manufacture, purchase, sale or distribution or possession of drug paraphernalia.

l. Expressed intent to continue illegal drug use, or failure to clearly and convincingly commit to discontinue drug use.

Conditions that could mitigate security concerns

40. Conditions that could mitigate security concerns include:

a. So much time has passed, or the behaviour was so infrequent, or it happened under such unusual circumstances that it is unlikely to recur or does not cast doubt on the clearance subject's current reliability, trustworthiness or good judgement.

b. The clearance subject is participating in an alcohol counselling or treatment program, has no history of previous treatment and relapse and is making satisfactory progress:

   i. The clearance subject has acknowledged their alcohol dependence or abuse and has successfully completed inpatient or outpatient alcohol counselling or rehabilitation along with any required aftercare.

   ii. The clearance subject has demonstrated a clear and established pattern of modified consumption or abstinence in accordance with treatment recommendations and adherence to a program, such as Alcoholics Anonymous or a similar organisation.

   iii. The clearance subject has received a favourable prognosis by a duly qualified medical professional or an accredited clinical social worker who is a staff member of a recognised alcohol treatment program.

c. A demonstrated intent not to abuse any drugs in the future, such as:

   i. disassociation from drug using associates and contacts

   ii. changing or avoiding the environment where drugs were used

   iii. an appropriate period of abstinence

   iv. a signed statement of intent with automatic review for cause of clearance for any violation.

d. Abuse of prescription drugs was after a severe or prolonged illness during which these drugs were prescribed and the abuse has since ended.

e. Satisfactory completion of a prescribed drug treatment program, including but not limited to, rehabilitation and aftercare requirements, without recurrence of abuse, and a favourable prognosis by a duly qualified medical professional or an accredited clinical social worker who is a staff member of a recognised drug treatment program.

Criminal history and conduct

Concerns

41. Criminal activity creates doubt about a person's judgement, reliability, trustworthiness, maturity and honesty. It calls into question a person's ability or willingness to comply with laws, rules and regulations.

Conditions that could raise a security concern and may be disqualifying

42. Conditions that could raise a security concern and may be disqualifying include:

a. A criminal offence, or multiple lesser offences, or a conviction in an Australian or foreign court, including a military court-martial, for a crime.

b. Discharge or dismissal from the Australian Defence Force or police force under adverse conditions.

c. Credible allegation or admission of criminal conduct, regardless of whether the person was formally charged, formally prosecuted or convicted.

d. The clearance subject is currently on parole or probation.

e. Violation of parole or probation, or failure to complete a court-mandated rehabilitation program.

f. Voluntary association with criminals.

Conditions that could mitigate security concerns

43. Conditions that could mitigate security concerns include:

a. So much time has elapsed since the criminal behaviour happened, or it happened under such unusual circumstances that it is unlikely to recur and does not cast doubt on the clearance subject's reliability, honesty, trustworthiness or good judgement.

b. The person was pressured or coerced into committing the act and those pressures are no longer present in the person's life.

c. Persuasive evidence that the person did not commit the offence or the conviction for the offence was subsequently overturned.

d. There is evidence of successful rehabilitation, including the passage of time without recurrence of criminal activity, evidence of remorse or restitution, job training or higher education, good employment record or constructive community involvement.

Security violations

Concerns

44. Deliberate or negligent failure to comply with procedures, rules and regulations for protecting sensitive or security classified information, including on ICT systems, raises doubt about a clearance subject's trustworthiness, judgement, reliability or willingness and ability to safeguard such information, and is a serious security concern.

45. ICT systems include computer hardware, software, firmware and data used for the communication, transmission, processing, manipulation, storage or protection of security classified information.

Conditions that could raise a security concern and may be disqualifying

46. Conditions that could raise a security concern and may be disqualifying include:

a. The unauthorised:

i. viewing

ii. disclosing

iii. collecting

iv. storing

v. handling

vi. destroying

vii. manipulating

viii. modifying

of sensitive or security classified information.

b. Deliberate disregard of entity procedures or guidelines for the handling, use and storage of sensitive or security classified information.

c. Copying sensitive or security classified information in a manner designed to conceal or remove classification or other document control markings.

d. Viewing or downloading information from a secure system beyond the clearance subject's need to know.

e. Any failure to comply with rules for the protection of sensitive or security classified information.

f. Negligence or lax security habits that persist despite counselling by management.

g. Failure to comply with rules or regulations that result in damage to national security, regardless of whether it was deliberate or negligent.

h. Illegal or unauthorised:

   i. entry into any ICT system

   ii. modification

   iii. destruction

   iv. manipulation

   v. denial of access

   to information, software, firmware or hardware in an ICT system.

i. Use of any ICT system to gain unauthorised access to another system or to a compartmented area within the same system.

j. Downloading, storing or transmitting security classified information on or to any unauthorised software, hardware or ICT system.

k. Unauthorised use of a government or other ICT system.

l. Introduction, removal or duplication of hardware, firmware, software or media to or from any ICT system without authorisation, when prohibited by rules, procedures, guidelines or regulations.

m. Any misuse of ICT, whether deliberate or negligent, that results in damage to national security.

n. Misuse of both government and private information and ICT systems are of concern.

Conditions that could mitigate security concerns

47. Conditions that could mitigate security concerns include:

a. So much time has elapsed since the behaviour, or it has happened so infrequently or under such unusual circumstances, that it is unlikely to recur and does not cast doubt on the clearance subject's current reliability, honesty, trustworthiness or good judgement.

b. The clearance subject responded favourably to counselling or remedial security training and now demonstrates a positive attitude towards the discharge of security responsibilities.

c. The security violations were due to improper or inadequate training.

d. The misuse was minor and done only in the interest of a bona fide emergency or operational imperative when no other timely alternative was readily available.

e. The conduct was unintentional or inadvertent and was followed by a prompt, good faith effort to correct the situation and notify a supervisor.

Emotional and mental health issues

Concerns

48. Certain emotional, mental and personality conditions can impair judgement, reliability or trustworthiness. A formal diagnosis of a disorder is not required for there to be a concern under this guideline.

49. A duly qualified mental health professional (eg clinical psychologist or psychiatrist) employed by or acceptable to and approved by the entity, must be consulted when evaluating potentially disqualifying and mitigating information under this guideline.

50. No negative inference concerning the standards in these guidelines may be raised solely based on seeking mental health counselling.

Conditions that could raise a security concern and may be disqualifying

51. Conditions that could raise a security concern and may be disqualifying include:

    a. Behaviour that casts doubt on a clearance subject's judgement, reliability or trustworthiness that is not covered under any other guideline, including emotionally unstable, irresponsible, dysfunctional, violent, paranoid or bizarre behaviour.

    b. An opinion by a duly qualified mental health professional that the clearance subject has a condition not covered under any other guideline that may impair judgement, reliability or trustworthiness.

    c. The clearance subject has failed to follow treatment advice related to a diagnosed emotional, mental or personality condition, for example failure to take prescribed medication.

Conditions that could mitigate security concerns

52. Conditions that could mitigate security concerns include:

    a. The identified condition is readily controllable with treatment and the clearance subject has demonstrated ongoing and consistent compliance with the treatment plan.

    b. The clearance subject has voluntarily entered a counselling or treatment program for a condition that is amenable to treatment and the clearance subject is currently receiving counselling or treatment with a favourable prognosis by a duly qualified mental health professional.

    c. Recent opinion by a duly qualified mental health professional employed by or acceptable to and approved by the entity seeking the clearance that a clearance subject's previous condition is under control or in remission and has a low probability of recurrence or exacerbation.

    d. The past emotional instability was a temporary condition (eg one caused by death, illness, or marital break-up), the situation has been resolved, and the clearance subject no longer shows indications of emotional instability.

    e. There is no indication of a current problem.

Annex B. Variation of Special Minister of State's Determination 2018/27 for a Minister's electorate officer

1. The Special Minister of State Determination 2018/27 requires that staff of Ministers employed under Part III of the *Members of Parliament (Staff) Act 1984* obtain and maintain a Negative Vetting Level 2 security clearance. Under the Determination, a Minister's Chief of Staff may request a variation of the security clearance requirement from the Secretary of the Attorney-General's Department.
2. The Secretary, Attorney-General's Department will consider a request to vary the requirement for a Negative Vetting Level 2 security clearance following endorsement by the portfolio department.

Annex B Table 1 Possible variations to Members of Parliament staff security clearance requirements

Staff	Information access	Security clearance variation
Electorate officers employed by an NSC Minister	SECRET or TOP SECRET	No variation. Negative Vetting Level 2 security clearance required
	OFFICIAL, OFFICIAL: Sensitive or PROTECTED	Variation to Baseline security clearance may be sought
Electorate officers employed by a non-NSC Minister	TOP SECRET	No variation. Negative Vetting Level 2 security clearance required
	SECRET	Variation to Negative Vetting Level 1 security clearance may be sought
	OFFICIAL, OFFICIAL: Sensitive or PROTECTED	Variation to Baseline security clearance may be sought

Minister's Chief of Staff request for variation

I certify that Name of electorate officer is an electorate officer for Minister's name and 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 Level 2 security clearance.

Name of Chief of Staff	Phone number	Signature	Date
			/ /

Forward request to the Chief Security Officer or delegate of the portfolio department

Portfolio department endorsement of request

Name of portfolio department

I endorse the request to vary the requirement for a Negative Vetting Level 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

Send to: Protective Security Policy Section, Attorney-General's Department, 3-5 National Circuit, BARTON ACT 2600

Approval of request

As the delegate for the Secretary, Attorney-General's Department, I vary the requirement for the above mentioned electorate officer to be security cleared to Negative Vetting Level 2, subject to them undergoing (tick whichever is applicable):

☐ Baseline
☐ Negative Vetting Level 1
☐ Variation not approved - Negative Vetting Level 2 required

Name of approving officer	Position of approving officer	Date
		/ /

Send to: Ministerial and Parliamentary Services, Department of Finance, Parkes Place, PARKES ACT 2600

Annex C. What is procedural fairness

1. Procedural fairness is concerned with the procedures used by a decision maker, rather than the actual outcome reached – it is a matter of administrative law. It requires a fair and proper procedure be used when making a decision. A decision maker who follows a fair procedure is more likely to reach a fair and correct decision. The two primary rules of procedural fairness are:
   a. the hearing rule, which requires a person be given an opportunity to be heard and express their views to a decision maker
   b. the bias rule, which requires a decision maker to be impartial.
2. 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.

Procedural fairness and security clearance decisions

3. To comply with administrative law principles, 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.
4. As part of the security clearance decision-making process and in accordance with the hearing rule, where an adverse decision is proposed, the Attorney-General's Department recommends that 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 recommended that vetting agencies ensure that the clearance subject:
   a. 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 a 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
   b. is provided with a reasonable opportunity to consider their position and prepare a response
   c. have their reply considered by the delegate before the decision is made.
5. The bias rule requires that a delegate making a security clearance decision:
   a. does not have an interest (either direct or indirect) in the matter being decided
   b. does not bring, or appear to bring, a biased or prejudiced mind to making the decision.
6. A delegate must be impartial. Vetting agencies must maintain processes to ensure application of the bias rule to comply with administrative law principles.

How does procedural fairness apply to a clearance subject who may be negatively affected by a delegate's decision?

7. If a clearance subject is negatively affected by a delegate's decision they can expect that the assessing officer and delegate will follow the rules of procedural fairness before reaching a conclusion. In particular, a clearance subject is entitled to:
   a. being told the case to be met (eg 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 (any negative or prejudicial information relating to the clearance subject must be disclosed to the extent possible consistent with national security)
   b. an opportunity to reply to the case to be met by a written reply or submission or, in very exceptional circumstances, a delegate may determine it appropriate that a face-to-face meeting be facilitated.

8. In submitting a reply to the delegate, a clearance subject may:
    a. deny the allegations
    b. provide evidence they believe disproves the allegations
    c. explain the allegations or present an innocent explanation
    d. provide details of any special circumstances they believe need to be taken into account.

How does procedural fairness apply to an assessing officer?

9. An assessing officer 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, an assessing officer must:
    a. consider all submissions made by a clearance subject
    b. take into account only relevant information
    c. ensure that any recommendation made is based on evidence that is relevant and supports the recommendation
    d. act fairly and impartially
    e. conduct the clearance process without unnecessary delay
    f. ensure that a full record of the clearance process has been made.

How does procedural fairness apply to the delegate?

10. 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. a clearance subject has been provided with an opportunity to be heard to make submissions if this has not already occurred
    b. they act fairly and impartially, including ensuring there is no reasonable perception of bias on the part of the delegate.

Annex D. Review of decisions

1. The denial or granting of a security clearance, with or without specific clearance maintenance requirements, is an administrative decision and is reviewable. The avenues for review vary depending on the applicable vetting agency, sponsoring entity and the status of the clearance subject.

Administrative review process by employer

Employer	Administrative review process
APS employees	Primary review by the relevant vetting agency – an employee can seek an initial review conducted by the vetting agency. The employee has 120 days from notification of the security decision to request a review under regulation 5.24(1) of the Public Service Regulations 1999. Secondary review by the Merit Protection Commissioner – an employee can seek an independent review if they are dissatisfied with a decision arising from the vetting agency's review or have been advised that the matter is not reviewable. An employee has 60 days from the time they are advised of the decision of the relevant vetting agency's review to make an application for review by the Merit Protection Commissioner under regulation 5.29(1) of the Public Service Regulations 1999. An employee seeking review must lodge their application with the vetting agency. The agency has 14 days to forward the application to the Merit Protection Commissioner with all of the relevant paperwork from the primary review. Employees may also lodge a complaint with the Commonwealth Ombudsman. An Ombudsman will generally only investigate a complaint if other review processes have been completed within the relevant agency. If an employee is dissatisfied with the Ombudsman's decision whether to investigate a complaint, they can seek an internal review of the decision within 3 months.
Australian Defence Force members	Members may seek an internal review via the procedures outlined in Defence Complaints and Resolution Manual that is available to Australian Defence Force members. Australian Defence Force members can also seek review by the Defence Force Ombudsman.
Non-APS employees	Employees may have access to internal review procedures set by the relevant vetting agency. Employees may also lodge a complaint with the Commonwealth Ombudsman. An Ombudsman will generally only investigate a complaint if other review processes have been completed within the relevant agency. If an employee is dissatisfied with the Ombudsman's decision whether to investigate a complaint, they can seek an internal review of the decision within 3 months.

2. A secondary review by the Merit Protection Commissioner cannot reverse a decision made by the delegate, under regulation 5.28 of the Public Service Regulations 1999. Instead, under the regulations the Commissioner must make a recommendation to the relevant authorised vetting agency. Under regulation 5.32, the vetting agency may confirm the action, vary it or set the action aside and substitute a new action in response to the recommendation. The agency must advise the Merit Protection Commissioner of its decision. If the Merit Protection Commissioner is not satisfied with the vetting agency's response, subsection 33(6) of the *Public Service Act 1999* allows for the matter to be reported to the agency's minister, the Prime Minister and the Parliament.
3. The clearance subject may appeal in the Administrative Appeals Tribunal against any assessment or any decision made as a result of the ASIO assessment. The subject must be advised in writing within 14 days of any adverse or qualified ASIO assessment, taking into account any restrictions imposed by an Attorney-General's Certificate and provided with a copy of the unclassified security assessment and statement of grounds that sets out the case against them. 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.
4. The Attorney-General's Department recommends vetting agencies 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.
5. The clearance subject may also make a formal complaint to:

a. the Privacy Commissioner, if they feel there was a breach of the *Privacy Act 1988* in the way information was handled

b. 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.

6. The clearance subject may also seek judicial review of a vetting decision in the Federal Court of Australia or High Court of Australia under section 39B of the *Judiciary Act 1903* or section 75(v) of the Constitution.

Annex E. Digital footprint checks framework

Purpose

1. This framework assists vetting agencies to conduct digital footprint checks in a consistent manner. It also helps vetting agencies 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.
2. This digital footprint check framework sets out:
   a. a definition of publicly accessible data
   b. the minimum required checks
   c. considerations for identifying and assessing online information.
3. 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.
4. 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.
5. The Attorney-General's Department, in consultation with the AGSVA and the Vetting Officers Community of Practice, has developed the framework to align with the requirements of the PSPF.

Publicly accessible data

6. **Requirement 3cii** of the PSPF policy: Eligibility and suitability of personnel mandates that vetting agencies conduct personnel security checks for all clearance levels (Baseline to Positive Vetting, inclusive) including a publicly accessible digital footprint check.
7. Online publicly accessible information refers to data that has been published online and is available publically. This includes information obtained by virtue of general memberships, accounts on online social platforms or websites that are available to anyone.
8. 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.
9. Publicly accessible data collected about an individual may be defined as personal information for the purposes of the *Privacy Act 1988*. Vetting agencies are responsible for ensuring that digital footprint check policies and procedures[3] accord with the information requirements in the *Privacy Act 1988*, the *Archives Act 1983* and any agency specific legislation.

Minimum required checks

10. 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 checks required to establish a digital footprint are an open internet search check and social media check as detailed in **Annex E Table 1**.
11. To conduct these checks effectively, vetting agencies need sufficient personal information about the clearance subject. This may include details of online aliases and accounts.[4] The level of information

[3] Including the management and storage of online information collected through digital footprint checks.
[4] 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.

requested from a clearance subject and the extent of checks against this information should be proportionate to the level of clearance, the relevant background check period and any identified security concerns or risks about the clearance subject.

Annex E Table 1 Minimum digital footprint checks

Check	Rationale	Recommended minimum search parameters
Open search check	An open search engine enables a wide screening of online data that may provide information on a clearance subject not captured in other security vetting checks. The Attorney-General's Department recommends that vetting agencies check the clearance subject's details within an open search engine to screen for any publicly accessible information relating to the clearance subject that is relevant to establishing their integrity and assessing their suitability to hold an Australian Government security clearance, including: a. content generated by or attributable to the clearance subject b. financial, professional and personal interests c. key associates or influences d. legal or administrative proceedings e. media relating to clearance subject f. any other data relevant to the clearance subject's integrity.	**Search terms:** a. clearance subject's full name b. clearance subject's email address(es) c. account names, aliases or handles provided by the clearance subject (for large volume search returns it may be necessary to limit the search to a geographical location). **Time**: a. relevant background check period (for large volume search returns it may be necessary to sample relevant returns). **Search engines:** a. any open search engine (eg Google, Bing, Internet Archive).
Social media check	Online social media relating to the clearance subject can provide information about their online behaviour and social networks. The Attorney-General's Department recommends that vetting agencies screen social media accounts and pages relating to the clearance subject for any publicly accessible information that is relevant to establishing their integrity and assessing their suitability to hold an Australian Government security clearance, including: a. posted content b. 'shared' and 'liked' content (this should be viewed with caution, however, may be useful if consistent with other information known about, or posts made by, the clearance subject) c. participation in online communities and interest groups d. pages or accounts followed e. networking and interactions with other online persons or accounts. 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.	**Search terms**: a. clearance subject's full name b. clearance subject's email address(es) c. account names, aliases or handles provided by the clearance subject (for large volume search returns it may be necessary to limit the search to a geographical location). **Time**: a. relevant background check period (for large volume search returns it may be necessary to sample relevant returns). **Social media platforms**: a. Facebook, Instagram, Twitter b. any platforms the clearance subject has disclosed in the vetting process c. any platforms identified in the open search check.

12. 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.

Identifying and assessing online information

13. As an element of security vetting, the digital footprint check is conducted against the factor areas of the Personnel Security Adjudicative Guidelines. The check's purpose is to collect information to support the assessment of the clearance subject's suitability to hold a security clearance and to establish their integrity. The factor areas of the guidelines assist in focusing digital footprint checks against relevant criteria.

14. The Attorney-General's Department recommends that vetting agencies corroborate and verify the integrity of the information if the digital footprint check identifies information of security concern. Where there are remaining issues in attributing information to the clearance subject, it may be warranted to raise this with the clearance subject and provide them with an opportunity to clarify or provide further information.

15. Recommendations on a security clearance outcome should not rely solely on information collected through a digital footprint check.

16. The Attorney-General's Department recommends vetting agencies 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 (eg close associates of foreign nationality, significant life events and international travel or employment), should be resolved by the vetting agency.

Online behaviour

17. Posts, photos and other online activities are all online behaviours. Some online behaviours may be indicators of security concern that require further investigation or consideration in the vetting process. Some examples of online behaviours that may be of security concern are described in **Annex E Table 2**.

Annex E Table 2 Examples of online behaviours that may be of security concern

Online behaviours	Relevant 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 wilfully contravening of rules or regulations governing the handling of sensitive 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.

18. It can be difficult to establish the context of some online behaviour. However, vetting officers 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. For example, further investigation may identify additional context such as a clearance subject following controversial pages for research interest rather than personal loyalty, or posting comments that are difficult to interpret without knowledge of a community's culture or influences. This additional context could mitigate the concerns identified against the relevant factor areas.

Keeping records of online information

19. 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[5]) 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.

20. The Attorney-General's Department recommends that vetting agencies comprehensively document information obtained through a digital footprint check because of the changing nature of online information. Information must have a relevant bearing on a clearance subject's suitability to hold a security clearance, including screenshots and direct links where possible.

[5] Sensitive personal information about a third party can only be collected if the third party consents to the collection. For information, see the Office of the Australian Information Commissioner Australian Privacy Principle Guidelines.