13 Ongoing assessment of personnel

A. Purpose

1. This policy describes how entities maintain confidence in their personnel's ongoing suitability to access Australian Government resources, and manage the risk of malicious or unwitting insiders. It is critical that entities are aware of changes in their employees' circumstances and workforce behaviours. This awareness is facilitated by effective information sharing and a positive security culture, recognising that security is everyone's responsibility.
2. Effectively assessing and managing ongoing suitability ensures that entities' personnel, including contractors, continue to meet eligibility and suitability requirements established at the point of engagement. This includes continuing to meet an appropriate standard of integrity and honesty.

B. Requirements

B.1 Core requirement

Each entity must assess and manage the ongoing suitability of its personnel and share relevant information of security concern, where appropriate.

3. Accountable authorities are responsible for determining their entity's risk tolerance and managing the security risks of their entity, including as they relate to the ongoing suitability of personnel to access Australian Government resources.
4. Sponsoring entities and authorised vetting agencies play a critical role in assuring ongoing suitability of personnel occupying positions that require access to security classified resources or additional levels of assurance. The supporting requirements detail the respective responsibilities of sponsoring entities and vetting agencies for assessing the ongoing suitability of security cleared personnel.

B.2 Supporting requirements

Supporting requirements for ongoing assessment of personnel

#	Supporting requirements
Requirement 1. Security clearance maintenance Note i	a. Sponsoring entities **must** actively monitor and manage the ongoing suitability of their security cleared personnel, including: i. collecting, assessing and sharing information of security concern ii. conducting annual security checks with all security cleared personnel iii. monitoring compliance with, and managing risk in relation to, clearance maintenance requirements for security clearance holders granted a conditional security clearance and reporting non-compliance to the authorised vetting agency, and iv. reviewing eligibility waivers at least annually, before revalidation of a security clearance, and prior to any proposed position transfer. b. Vetting agencies **must**: i. share information of security concern about security clearance holders with sponsoring entities ii. assess and respond to information of security concern about security clearance holders, which includes reports from sponsoring entities, and iii. for conditional security clearances, review conditions annually iv. review the clearance holder's eligibility and suitability to hold a security clearance, where concerns are identified (review for cause).

#	Supporting requirements
Requirement 2. Security clearance revalidation	Vetting agencies **must** reassess a clearance holder's eligibility and suitability to hold a security clearance by: a. considering their integrity (ie the character traits of maturity, trustworthiness, honesty, resilience, tolerance and loyalty) in accordance with the Personnel Security Adjudicative Guidelines (see the PSPF policy: Eligibility and suitability of personnel Annex A) b. revalidating minimum personnel security checks for a security clearance outlined below, and c. resolving any doubt in the national interest.

Minimum requirements for revalidation of security clearances

Check	Security Clearance Level			
	Baseline Vetting	**Negative Vetting 1**	**Negative Vetting 2**	**Positive Vetting**
Revalidation [Note ii] undertaken at least every:	15 years	10 years	5 to 7 years	5 to 7 years
Updated personal particulars	✓ Required	✓ Required	✓ Required	✓ Required
	Entities **must** confirm any changes to a clearance holder's personal particulars using identification documents verified with the issuing authority by using the Document Verification Service for Australian-issued primary identification documents.			
Background assessment covering period since the initial clearance or last revalidation	✓ Required	✓ Required	✓ Required	✓ Required
Referee checks covering period since the initial clearance or last revalidation	✓ Required	✓ Required	✓ Required	✓ Required
Digital footprint check covering period since the initial clearance or last revalidation	✓ 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 assessment	Not required	✓ Required	✓ Required	✓ Required
Security interview	Not required	Not required	✓ Required	✓ Required
Psychological assessment	Not required	Not required	Not required	✓ Required

Supporting requirements notes:

[i] Additional security clearance maintenance for Positive Vetting clearance holders are contained in the Sensitive Material Security Management Protocol – Personnel Security – Positive Vetting Guidelines (SMSMP-PVG). The SMSMP-PVG is available to entity security advisors or upon request via the PSPF community on GovTEAMS.

[ii] A revalidation covers the period since the initial clearance or last revalidation was completed, unless there are significant security concerns that raise doubts about the previous assessment, or indication of an enduring pattern of behaviour.

C. Guidance

C.1 Assessing and managing ongoing suitability

5. The potential for insiders (employees, contractors and others with access to Australian Government resources) to betray the trust placed in them presents an enduring security risk. Insiders who compromise

security may be unwitting or malicious. Possible motives are complex and can be driven by a mix of personal vulnerabilities, life events and situational factors.

6. While pre-employment screening and security clearance vetting (as described in the PSPF policy: Eligibility and suitability of personnel) provide an assessment of a person's suitability at a point in time, ongoing awareness of changes in personnel's circumstances and workplace behaviours is essential to manage the risk of insider threat. The **core PSPF requirement on ongoing assessment of personnel** mandates entities assess and manage the ongoing suitability of their personnel. This means entities are responsible for ensuring their personnel remain suitable to access Australian Government resources for the entire period of their engagement.
7. Effective assessment of personnel's ongoing suitability relies on entities encouraging and facilitating reporting of concerns, as well as collating and assessing information on personnel from a range of sources, including their management and colleagues. The way entities assess and manage ongoing suitability will depend on:
   a. the type of personnel (employees and contractors, security clearance holders or uncleared personnel) within the entity
   b. their access to classified and unclassified Australian Government resources
   c. the entity's tolerance for security risks
   d. any risks that may be specific to the position
   e. the individual's personal risk profile.
8. **Table 1** identifies entity procedures to assess and manage the ongoing suitability of personnel. Some of these may be built into existing performance management procedures. The Attorney-General's Department recommends entities' procedures for assessing and managing the ongoing suitability of personnel include periodic employment suitability checks, as well as mechanisms to support reporting of concerns.

Table 1 Procedures for assessing and managing ongoing suitability

Procedure	Uncleared personnel [Note iii]	Security cleared personnel
Building personnel security into performance management. [Note iv]	✓ Minimum procedure for **core requirement**.	✓ Minimum procedure for **core requirement**.
Periodic employment suitability check. [Note v]	✓ Minimum procedure for **core requirement**.	✓ Minimum procedure for **core requirement**.
Annual security check. [Note vi]	Procedure recommended to support the **core requirement**.	✓ Minimum procedure for **Requirement 1a**.
Contact reporting obligations. [Note vii]	Procedure recommended to support the **core requirement**.	✓ Minimum procedure for **Requirement 1a**.
Security incident reporting and follow-up. [Note viii]	Procedure recommended to support the **core requirement**.	✓ Minimum procedure for **Requirement 1a**.
Collecting and assessing information on changes in personal circumstances. [Note ix]	Procedure recommended to support the **core requirement.**	✓ Minimum procedure for **Requirement 1a**.
Annual reviews of eligibility waivers. [Note x]	Not applicable, procedures not required.	✓ Minimum procedure for **Requirement 1a** for holders of a clearance subject to an eligibility waiver.
Monitoring compliance with clearance conditions. [Note xi]	Not applicable, procedures not required.	✓ Minimum procedure for **Requirement 1a** for holders of a conditional security clearance.
Positive Vetting maintenance obligations in accordance with the SMSMP-PVG.	Not applicable, procedures not required.	✓ Minimum procedure for **Requirement 1a** for Positive Vetting holders.

Table 1 notes:

[iii] Entities may choose to apply assurance measures for security cleared personnel to all entity personnel, based on the assessment of and tolerance for risk. Effective ongoing assessment of personnel may trigger consideration of other risks including fraud, corruption and breaches of legislation (including provisions in the *Public Service Act 1999*, eg the APS Code of Conduct). Note that, in the absence of an authorised vetting agency, entities will have to assess and manage security concerns for uncleared personnel themselves.
[iv] For guidance on building personnel security into performance management, see C.1.2.
[v] For guidance on periodic employment suitability checks, see C.1.3.
[vi] For guidance on annual security checks, see C.1.4.
[vii] For guidance on contact reporting obligations, see C.1.5.
[viii] For guidance on security incident reporting and follow-up, see C.1.6.
[ix] For guidance on collecting and assessing information on changes in personal circumstances, see C.1.7.
[x] For guidance on annual reviews of eligibility waivers, see C.1.9.
[xi] For guidance on monitoring compliance with clearance conditions, see **Error! Reference source not found.**.

C.1.1 Security clearance maintenance

9. Security clearance maintenance requirements are in addition to ongoing suitability measures that apply for all personnel.

10. Ensuring the ongoing eligibility and suitability of security cleared personnel to hold an Australian Government security clearance is the joint responsibility of vetting agencies, the sponsoring entity and the individual clearance holder. **Requirement 1** details the respective roles and responsibilities of vetting agencies and sponsoring entities for security clearance maintenance; this includes specific clearance maintenance requirements for holders of conditional security clearances and clearances subject to eligibility waivers. For security cleared personnel:

    a. sponsoring entities are responsible for assessing how information relates to an entity's security risks, as well as a person's suitability for employment by the entity. This is particularly relevant where there are entity-specific employment requirements, such as a zero-tolerance drug and alcohol policy.

    b. authorised vetting agencies are responsible for assessing how information relates to an individual's eligibility and suitability to hold a clearance.

11. The **core PSPF requirement on ongoing assessment of personnel** mandates that entities share relevant information of security concern. The assessment of whether information is relevant or of security concern can only be made by the entity assessing that concern. **Requirement 1** clarifies that sponsoring entities and vetting agencies must share all information relating, or appearing to relate, to the ongoing suitability of personnel so the entity receiving the information can determine whether it is relevant.

C.1.2 Performance management

12. Entity performance management programs provide an avenue for supervisors and line managers to assess and report on the ongoing performance of personnel. Performance management programs may also be used for the assessment and management of ongoing suitability, including identifying personnel who display behavioural concerns such as disregard for entity security procedures.

13. Entities are encouraged to embed security considerations into their annual performance appraisals by seeking confirmation from:

    a. individuals that they have reported any change of circumstances, such as:

        i. changes to details provided during the pre-employment screening (eg criminal charges)

    b. individuals that they have reported any

        i. suspicious, ongoing, unusual or persistent contact with foreign and Australian nationals who are seeking information that they do not need to know, as well as suspicious, ongoing, unusual or persistent incidents (eg such as social media contact)

        ii. real or perceived conflicts of interest

    c. line managers that there are no unreported security concerns about the individual.

14. The Attorney-General's Department recommends entities provide line managers with guidance on identifying behaviours of concern and engaging in effective conversations about personnel security within the context of performance management. Examples include confirming compliance with mandatory security awareness training, and ensuring understanding of reportable incidents and the contact reporting scheme. It is also important to identify gaps in knowledge about security, particularly where specialist knowledge or training is required to address entity-specific risks or in relation to compartmental briefings.
15. Where security concerns are identified as part of performance management, entities are encouraged to undertake additional employment suitability checks to assess whether the concerns are relevant to the person's ongoing suitability to access Australian Government resources. Identifying security concerns may trigger incident reporting obligations under the PSPF Governance core requirements.
16. For security clearance holders, security concerns could affect their eligibility and suitability to hold a security clearance. Where concerns are identified, the Attorney-General's Department recommends that clear processes be developed for line managers to provide this information to security advisors responsible for entity personnel security, and for the security advisors to provide the information to the vetting agency.
17. Central human resources areas may also have knowledge of performance concerns through line manager reporting or analysis of employment data, such as unexplained absences or unplanned leave. These performance concerns could be indicators of other personal issues that can lead to security concerns, for example alcohol or drug abuse, or financial difficulties. The Attorney-General's Department recommends developing procedures and providing guidance for human resources areas to support information sharing arrangements and assist with identifying and communicating information.
18. The relationship between performance issues and security concerns is complex. It is important that entities do not misuse the security clearance process to address performance issues (eg referring security concerns to the vetting agency in the hope that a security clearance may be withdrawn). Performance management processes or investigations do not preclude entities from providing the authorised vetting agency with information about security relevant performance issues.

C.1.3 Periodic employment suitability checks

19. Pre-employment screening provides the foundation of good personnel security and reduces the risk of an insider harming business operations. Pre-employment screening checks can be repeated periodically over the course of a person's employment to inform an assessment of ongoing suitability. The Attorney-General's Department recommends entities determine the frequency of these periodic employment suitability checks based on the entity's risk profile as well as specific risks associated with the position, any associated enabling legislation and the entity's operating environment. **Table 2** describes a range of recommended periodic employment suitability checks.

Table 2 Periodic employment suitability checks

Check	Description
Updating personal particulars	Personnel may be asked to periodically update their personal particulars. This could include: a. updating residential address history b. updating any qualifications c. updating employment history for contractors. It may be useful to verify changes to personal particulars through independent sources, including the Document Verification Service if there are changes to Australian-issued primary identification documents.
Confirming adherence to, or completion of, engagement conditions	Where conditions have been placed on an initial or continuing engagement (eg gaining Australian citizenship), confirm those conditions have been met within specified timeframes.

Check	Description
National police check	If police checks are conducted less frequently than every 10 years, convictions under the Spent Convictions Scheme may not be included. The Attorney-General's Department recommends a police records check at least every 10 years; the frequency may be increased for high-risk positions or personnel. The Spent Convictions Scheme applies to spent convictions where a waiting period has passed and the individual in question has not re-offended. The conditions that apply to convictions for a Commonwealth, state, territory or foreign offence are: a. it has been 10 years from the date of the conviction (or 5 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 (5 years for juvenile offenders) waiting period d. a statutory or regulatory exclusion does not apply. The scheme also protects convictions that have been set aside or pardoned under Part VIIC of the *Crimes Act 1914*. An individual whose conviction is protected does not have to disclose the conviction to any person, including a Commonwealth authority.
Credit history check	Where an entity's risk assessment deems that it requires assurance of a person's financial situation, periodic financial screening (including a credit history check) may provide indicators of financial stressors.
Conflict of interest declaration	APS employees have an obligation under section 13 of the *Public Service Act 1999* to disclose and take reasonable steps to avoid actual or perceived conflicts of interest. The Attorney-General's Department recommends reconfirming with personnel that any changes in their circumstances have not resulted in any actual or perceived conflict of interest. For further advice, see the Australia Public Service Commission publication Conflict of interest.
Confidentiality agreement	Periodic completion of confidentiality or non-disclosure agreements helps remind personnel of their ongoing confidentiality obligations.
Other entity-specific checks	Personnel who are in positions subject to entity-specific pre-employment checks may have these checks periodically repeated. Examples of entity-specific checks include drug and alcohol testing, financial probity checks and psychological assessments. For information, see the Australia Public Service Commission publication Conditions of engagement.

C.1.4 Annual security check

20. **Requirement 1aii** mandates that entities conduct an annual security check with all security cleared personnel. An annual security check addresses:

    a. the person's compliance with general security clearance obligations, as well as any conditions associated with a conditional security clearance. General security clearance obligations for clearance holders include compliance with entity security procedures, in particular:

        i. reporting:

            A. changes in circumstances

            B. security incidents

            C. suspicious, ongoing, unusual or persistent contact with foreign and Australian nationals who are seeking information that they do not need to know, as well as suspicious, ongoing, unusual or persistent incidents (eg such as social media contact)

        ii. completing security awareness training

    b. the person's workplace behaviours to identify behaviours of concern.

21. An annual security check provides an opportunity to discuss any identified behavioural concerns, improve awareness and understanding of security obligations, and reinforces a positive security culture.

22. The Attorney-General's Department notes that line managers are well placed to conduct an annual security check as they are likely to have the best knowledge of their personnel's behaviour. Where appropriate,

checks may be conducted in consultation with a security advisor or an appropriate representative from the entity's human resources area. This may be particularly relevant where clearance conditions exist.

23. Entities may include the annual security check as part of their annual performance management process or as a stand-alone requirement. The annual security check does not replace an entity's responsibility to monitor and evaluate ongoing suitability through performance management, including code-of-conduct investigations.

24. If the sponsoring entities' annual security check identifies any security concerns about a security clearance holder, **Requirement 1a** mandates entities share that with the relevant authorised vetting agency in addition to reporting any changes in circumstances, security incidents, and suspicious, ongoing, unusual or persistent contact reports as they occur.

25. Personnel holding a Positive Vetting security clearance are subject to additional requirements for annual security appraisals. These are set out in the SMSMP-PVG.

C.1.5 Contact reporting obligations

26. Reporting suspicious, unusual or persistent contacts and incidents, as well as contact with foreign and Australian nationals who are seeking information that they do not need to know, is one means to address the enduring threat that espionage poses to the Australian Government.

27. Contact reporting obligations are set out in the PSPF policy: Management structures and responsibilities. These reporting obligations are relevant when assessing ongoing suitability of personnel. Reports of suspicious, ongoing, unusual or persistent contacts may inform an entity's risk assessment in relation to an individual, a position or a work area. Non-compliance with contact reporting obligations is a security concern. In accordance with **Requirement 1a**, sponsoring entities are required to share information about suspicious, unusual or persistent contacts with the authorised vetting agency in addition to forwarding reports to ASIO.

C.1.6 Security incident reporting and follow up

28. Managing security incidents and investigations helps monitor security performance, identify inadequacies in security procedures and detect security risks in order to implement appropriate treatments. At the individual level, a history of security incidents (regardless of their individual scale or significance) may raise questions about a clearance holder's suitability to retain access to Australian Government resources.

29. The PSPF policy: Management structures and responsibilities **Requirement 2** mandates that entities establish procedures for managing security incidents. In accordance with **Requirement 1a**, entities must share information on security incidents relating to a security clearance holder with the relevant authorised vetting agency.

C.1.7 Collecting and assessing information on changes in circumstance

30. Reporting changes in circumstance helps entities assess personnel security risk based on current and relevant information. Early identification of changes in risk profiles can prevent smaller issues from becoming larger problems. At the individual level, this means encouraging and enabling self-reporting of changes in circumstance by personnel. At the entity level, this means having effective procedures to collect, assess and manage reported changes in circumstances.

31. Vetting agencies grant security clearances after careful consideration of the whole-of-person assessment at the time of granting the clearance. However, as circumstances change over time, this may affect ongoing eligibility and suitability of a person to hold a clearance. Changes in circumstances may:

    a. increase a person's vulnerability to coercion

    b. lead to deliberate breaches of security, fraud or corruption

    c. be used by foreign governments, commercial organisations, issue-motivated groups, criminal organisations or others to induce personnel into providing information or goods belonging to the government.

32. In accordance with **Requirement 1a**, sponsoring entities must share information on any changes in circumstances of a clearance holder with the relevant authorised vetting agency. **Table 3** provides guidance on entity responsibilities for assessing and managing changes in circumstances.

Table 3 Guidance on reporting changes in circumstance

Reporting obligation	Description
What changes in circumstance to report	Changes in circumstance are reportable where there are: a. changes of name/identity (gender) b. changes in significant relationships c. changes in address or share-housing arrangements d. entering into, or ceasing, a relationship (marriage, civil union or de facto) e. changes in citizenship or nationality f. changes in financial circumstances g. changes in health or medical circumstances h. changes in criminal history, police involvement and association with criminal activity i. involvement or association with any group, society or organisation j. disciplinary actions k. drug or alcohol problems l. residence in, or visits to, foreign countries m. relatives residing in foreign countries n. suspicious, persistent or unusual contacts (for information, see section C.1.5 – Contact reporting obligations) o. any other significant changes in circumstance. This list is not exhaustive. If personnel are uncertain whether the information is relevant, report it to the line manager, Chief Security Officer or a security advisor responsible for personnel security.
How to report changes in circumstances	The Attorney-General's Department recommends entities: a. make clear the process and responsible area within their entity where clearance subjects report any change in circumstances b. require clearance holders to report all changes in circumstances to the identified area c. require line managers to report all changes in circumstances relating to their clearance holder personnel, regardless of whether they believe changes have been notified by the clearance subject d. encourage all staff to advise line managers of significant changes in circumstances (noting this may not always be appropriate). Under the PSPF policy: Management structures and responsibilities, entities must provide security awareness training and establish procedures for managing security incidents. Consistent with that policy, the Attorney-General's Department recommends security awareness training cover entity procedures to report changes in circumstance in a manner that enables, encourages and facilitates timely reporting.
Who reports changes in circumstances	Where personnel fall into more than one listed category, report in accordance with all applicable categories: a. Security clearance holders report changes in their circumstances b. Line managers and contract managers report any concerns with personnel they manage c. Human resources areas report any employment-related concerns or investigations, including those related to breaches of the Code of Conduct d. All personnel report concerns about other individuals where it may affect entity security. The Attorney-General's Department recommends consideration is given to ensuring personnel feel able to report concerns about their managers.
What to do with information on changes in circumstances	When an entity is advised about an individual's change in circumstances, the entity considers that information for the purposes of assessing and managing the ongoing suitability of that individual, and shares information of security concern, where appropriate. **Requirement 1a** mandates entities share all reports of changes in circumstances relating to clearance holders with the relevant authorised vetting agency, which may initiate actions in relation to the person's security clearance. The vetting agency will notify the sponsoring entity to allow it to manage any associated risks. Entities assess all reports of changes in circumstances to identify whether there are any security concerns for the entity, and respond to those concerns in accordance with entity procedure. If there

Reporting obligation	Description
	are potential security concerns as a result of changes in circumstances, there are different avenues that can be pursued by the sponsoring entity. These include: a. security investigations b. code-of-conduct investigations c. criminal investigations. Where an allegation of security concern is received, an investigation by the sponsoring entity or the vetting agency may validate the report. It is important that entities do not prejudice the person in question, as some claims can be malicious. For information, see the Australian Privacy Principle 10 – quality of personal information. Where a sponsoring entity's investigation brings to light any additional information of security concern, **Requirement 1a** mandates this information be shared with the relevant authorised vetting agency.

C.1.8 Monitoring compliance with conditional security clearances

33. Where there are ongoing concerns about a clearance subject's eligibility or suitability to hold a security clearance, but they are not sufficient to deny the clearance, an authorised vetting agency may, after consultation with the sponsoring entity, recommend clearance conditions to mitigate these concerns (see the PSPF Policy: Eligibility and suitability of personnel). If agreed by the sponsoring entity and clearance subject, the vetting agency may issue aconditional clearance.

34. **Requirement 1aiii** mandates that sponsoring entities monitor security clearance holders granted a conditional security clearance to ensure compliance with the conditions and manage any related risks. Sponsoring entities are also required to report any non-compliance to the authorised vetting agency. Some conditions may also specify a reporting regime to the vetting agency to ensure compliance. **Requirement 1bi** mandates that vetting agencies share information of security concern about security clearance holders with sponsoring entities. In the case of conditional security clearance holders, this information is essential for sponsoring entities to effectively identify and manage any risks related to the conditional security clearance.

C.1.9 Annual review of eligibility waivers

35. **Requirement 1aiv** mandates that sponsoring entities review security clearance eligibility waivers at least annually and before revalidation of a security clearance.

36. An eligibility waiver is role-specific, non-transferable, finite and subject to review. In other words, the waiver applies only while the clearance holder remains in the position for which the clearance was granted. The waiver does not follow the clearance holder to any other position without review. An eligibility waiver is not open ended and is subject to regular review to confirm that there is a continuing requirement for the waiver.

37. It is important that personnel with clearances subject to a waiver (as well as their line manager and, potentially, co-workers) are informed of the limitations and conditions of the security clearance. For information, see the PSPF policy: Eligibility and suitability of personnel.

C.1.10 Clearance maintenance for personnel on secondment or temporary assignment

38. The Attorney-General's Department recommends that entities explicitly agree on security clearance arrangements for personnel who are seconded, or are on temporary assignment, before the secondment or assignment commences. It may be appropriate to transfer sponsorship of the security clearance to the receiving entity for the period of the secondment or assignment (depending on the length of time and the level of access still required to the losing entity's resources). For information, see the PSPF policy: Separating personnel.

39. In accordance with **Requirement 1a**, the losing and receiving entities are required to share information of security concern about the clearance holder with each other and with the relevant authorised vetting agency. This includes concerns identified after the secondment or temporary assignment concludes.

C.2 Ongoing assessment of security cleared personnel

40. Only authorised vetting agencies can make a determination about an individual's eligibility and suitability to hold a security clearance. However, vetting agencies can only assess an individual's eligibility and suitability based on the information available to them – this is why the effective sharing of information of security concern is so important.

41. Sponsoring entities are the critical repositories of information about a clearance holder's current circumstances and are best placed to provide the most current security-related information to the authorised vetting agency. Vetting agencies can then fulfil their responsibilities under **Requirements 1bii** and **1biv** to assess and respond to information of security concern about security clearance holders. This includes reviewing the clearance holder's eligibility and suitability to hold a security clearance where concerns are identified through the review for cause process.

42. Effective information sharing over the life of a security clearance will also make it easier for clearance holders and vetting agencies to compile the necessary information to conduct a revalidation of a security clearance. Where changes in circumstances and other information relevant to determining a person's eligibility or suitability to hold a security clearance, have already been considered by the vetting agency at the time they occurred, these assessments can inform the vetting agency's determination at revalidation.

43. **Requirement 1bi** mandates that vetting agencies share information of security concern about security clearance holders with sponsoring entities. This allows sponsoring entities to manage risks related to the clearance holder's ongoing access to Australian Government resources.

C.2.1 Annual review of clearance conditions

44. **Requirement 1biii** mandates that for conditional security clearances, the vetting agency must review the conditions annually. This ensures the conditions remain appropriate and continue to mitigate the identified security concerns. As part of this review it may be necessary for the vetting agency to confirm with the sponsoring entity and clearance subject that the agreed conditions are still able to be met. Where security concerns relevant to the clearance conditions have changed, the vetting agency will need to reassess the clearance holder's suitability to hold a security clearance.

C.2.2 Review for cause

45. **Requirement 1biv** mandates that authorised vetting agencies review a clearance holder's eligibility and suitability to hold a security clearance where concerns are identified. This process is known as a review for cause. Concerns may arise from:

    a. advice from the clearance subject of a change in circumstances

    b. concern raised by the clearance subject's sponsoring entity

    c. a security incident involving the clearance subject

    d. non-compliance with clearance conditions

    e. other information or advice of concern received by the vetting agency about the clearance subject.

46. A review for cause may entail an investigation into specific security concerns in the context of the whole person, or may prompt bringing forward a full revalidation of the security clearance (see C.2.4). In conducting a review for cause, vetting agencies are encouraged to:

    a. assess if a review for cause is warranted

    b. check with the sponsoring entity whether an ongoing investigation is underway that might be compromised by the review for cause and negotiate how to proceed

    c. advise the clearance subject prior to starting any reviews for cause and provide the reasons for the review

    d. undertake the checks required to resolve the concerns that led to the initiation of the review for cause, for example:

        i. targeted checks to resolve an issue

ii. a full revalidation if the concerns are wide ranging

e. advise both the clearance subject and the sponsoring entity of the review for cause outcome.

C.2.3 ASIO-initiated review of ASIO security assessment

47. All security clearances at the Negative Vetting 1 level and above are subject to an ASIO security assessment. An authorised vetting agency may request an ASIO security assessment for a Baseline security clearance if there are any concerns that may impact on the national interest.

48. ASIO can initiate a new security assessment at any time in response to new information.

49. At any time, ASIO may provide preliminary advice to a Commonwealth entity regarding the subject of an ASIO security assessment pending the issue of that assessment.

50. Sub-section 39(2) of the *Australian Security Intelligence Organisation Act 1979* (ASIO Act) permits Commonwealth entities to take appropriate action (such as suspending a person's security clearance and preventing ongoing access to classified information) if the Commonwealth entity is satisfied, on the preliminary advice from ASIO, that it is necessary to take that action as a matter of urgency due to requirements of security. Section 39 of the ASIO Act requires that any such action is temporary, pending receipt of an ASIO security assessment. Other than pursuant to the exception contained in subsection 39(2),) the ASIO Act prevents Commonwealth entities from taking prescribed administrative action on the basis of preliminary advice from ASIO.

51. ASIO will liaise with the Commonwealth entity and the relevant vetting agency when intending to provide preliminary advice under section 39 of the ASIO Act, including where an ASIO review of an existing security assessment indicates security concerns.

52. There is no legislative mechanism for ASIO to provide preliminary advice to a State or authority of a State to enable the taking of temporary action to prevent a risk to security.

53. While it is within ASIO's functions to furnish security assessments directly on States or authorities of States under section 40(1)(b) of the ASIO Act, section 40(2)(a) stipulates that ASIO is prohibited from furnishing to a State or an authority of a State, otherwise than in the form of a security assessment any information concerning a person which ASIO knows is intended or likely to be used by the State or an authority of the State in considering prescribed administrative action (such as refusing to grant a security clearance).

C.2.4 Revalidations

54. Revalidation assesses a clearance holder's ongoing eligibility and suitability to hold a security clearance by repeating many of the checks undertaken to determine their initial suitability, and again considering the clearance holder's integrity in accordance with the Personnel Security Adjudicative Guidelines. For information, see the PSPF policy: Eligibility and suitability of personnel Annex A.

55. **Requirement 2** mandates that authorised vetting agencies reassess a clearance holder's eligibility and suitability to hold a security clearance at specified intervals, depending on the level of the security clearance. **Requirement 2** specifies that minimum required checks must cover the period since the initial clearance or last revalidation was completed. This is unless there are significant concerns about the previous assessment or security concerns that would warrant covering a period up to and including the initial checkable period.

56. Vetting agencies commence the revalidation process sufficiently before the due date so that the security clearance does not lapse. Where new security concerns are identified during the revalidation process, the allowed time may not be sufficient. **Requirement 1bi** requires vetting agencies to share information of security concern about security clearance holders with sponsoring entities including allowing the sponsoring entity to suspend or limit the clearance holder's access to Australian Government resources until the concerns are resolved.

The Attorney-General's Department recommends vetting agencies commence the revalidation of security clearances in accordance with **Table** 3 below. Where cases are complex or new security concerns are identified during the revalidation process, this may require additional time.

Table 4 Recommended timeframes for commencing revalidations

Security clearance level	Baseline	Negative Vetting 1	Negative Vetting 2	Positive Vetting
Recommended commencement of revalidation process	1-3 months prior to the expiry date of a security clearance	3-6 months prior to the expiry date of a security clearance	9-12 months prior to the expiry date of a security clearance	12-18 months prior to the expiry date of a security clearance

57.

58. The Attorney-General's Department recommends vetting agencies contact the sponsoring entity before commencing the revalidation of a security clearance to confirm the continuing security clearance requirements. Entities are responsible for identifying and recording positions that require a security clearance and the level of clearance required. In addition, entities must ensure each person working in an identified position has a valid security clearance issued by an authorised vetting agency. This responsibility extends to where a clearance holder's duties or role has changed. If a higher level clearance is required, a new clearance process will be necessary. For information, see the PSPF policy: Eligibility and suitability of personnel.

C.3 Information sharing

59. The **core PSPF requirement on ongoing assessment of personnel** mandates that entities share information of security concern, where appropriate. This includes sharing information between line managers, human resources areas and security advisors as well as sharing information between sponsoring entities and vetting agencies. This requirement is relevant to information sharing in relation to transfers of personnel, including temporary and permanent transfers within entities and to other entities. Information covered by this requirement includes all information relevant to an individual's ongoing eligibility and suitability for employment or to hold an Australian Government security clearance. Information sharing may be limited by legislation, including the Australian Privacy Principles and an entity's enabling legislation.

C.3.1 Consent

60. Sharing relevant information, even when it is sensitive personal information, does not breach an individual's privacy provided that informed consent is received and the information is used for the purpose for which consent was given. It is therefore critical that entities obtain informed consent from all personnel (existing and potential) to share sensitive personal information with other entities and vetting agencies for the purposes of assessing their ongoing eligibility and suitability. The Attorney-General's Department recommends that consent is obtained at key information collection points , such as pre-employment screening and application for a security clearance, and updated at reasonable intervals, such as when conducting periodic employment checks and revalidation of a security clearance.

61. In some circumstances, there is a reasonable expectation that personal information will be shared, such as when an individual's information is crucial to rectify a security incident.

C.3.2 Security culture and information sharing

62. A well-developed culture of security encourages information sharing by personnel about the risks to themselves and their colleagues. Information sharing is dependent on an entity's aim to help manage concerns with their personnel before they escalate into an incident. While the focus is on prevention, entities are encouraged to have a clear, published and consistently enforced security regime that investigates and penalises inappropriate conduct. For information, see the PSPF policy: Management structure and responsibilities.

D. Find out more

63. Other legislation, policies or contacts include:

    a. APSC Conditions of engagement

    b. APSC Conflict of interest

    c. Australian Government Public Data Policy Statement

d. Australian Privacy Principles

e. OAIC Notifiable Data Breaches Scheme

f. *Criminal Code Act 1995*

g. *Australian Security Intelligence Organisation Act 1979*.

D.1 Change log

Table 4 Amendments in this policy

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