

From: s 22(1)(a)(ii) on behalf of s22(1)(a)(ii)
To: s22(1)(a)(ii)
Subject: AFP National Guideline on Personnel Security [DLM=For-Official-Use-Only]
Date: Monday, 29 January 2018 2:17:14 PM

For-Official-Use-Only



AFP National Guideline on Personnel Security

Manager Security has issued a new instrument which has been published in the AFP Governance Instrument Framework.

This instrument outlines the obligations for:

- clearance subjects:
 - seeking and maintaining an AFP security clearance
 - AFP security reporting requirements.
- AFP appointees assessing a clearance subject's eligibility and suitability to hold and maintain an AFP security clearance.

All clearance subjects should be aware non-compliance with security clearance requirements are reported to AFP Executive through SAS Visual Analytics.

AFP personnel are encouraged to familiarise themselves with this instrument which can be accessed through the following link:

- [AFP National Guideline on personnel security](#)

The contact for any queries about this instrument is [Security](#).

This instrument **supersedes and revokes** the following instruments which are no longer part of the GIF:

- AFP National Guideline on personnel security vetting
- AFP National Guideline on security reporting.

To request an **archived** version of any of the instruments above, contact s 22(1)(a)(ii) @afp.gov.au with the instrument name, nominated date (to identify version(s) needed) and a reason for the request.

Regards,

SECURITY
PEOPLE, SAFETY & SECURITY
www.afp.gov.au



POLICING FOR
A SAFER AUSTRALIA

For-Official-Use-Only

1. Disclosure and compliance

This document is marked **For Official Use Only** and is intended for internal AFP use.

Disclosing any content must comply with Commonwealth law and the [AFP National Guideline on information management](#).

Compliance

This instrument is part of the AFP's professional standards framework. The [AFP Commissioner's Order on Professional Standards \(CO2\)](#) outlines the expectations for appointees to adhere to the requirements of the framework. Inappropriate departures from the provisions of this instrument may constitute a breach of AFP professional standards and be dealt with under Part V of the [Australian Federal Police Act 1979](#) (Cth).

2. Acronyms & definitions

Acronyms and terminologies are defined in the [AFP Security Glossary of Terms](#).

3. Guideline authority

This guideline was issued by Manager Security using power under s. 37(1) of the [Australian Federal Police Act 1979](#) (Cth) (the Act) as delegated by the Commissioner under s. 69C of the Act.

4. Introduction

This guideline outlines the obligations:

- for clearance subjects:
 - when applying for, or maintaining their security clearance
 - establishing personnel security measures required to protect the AFP's classified resources from intentional and unintentional misuse
 - to exercise security responsibility to support and protect AFP operations, in accordance with [AFP Commissioner's Order on Security \(CO9\)](#).
 - security reporting requirements
 - who receive a threat as a direct result of their AFP employment (BULWARK).
- for AFP appointees assessing a clearance subject's eligibility and suitability to:
 - hold and maintain a security clearance in accordance with the AFP and the [Australian Government Protective Security Policy Framework \(PSPF\)](#).
 - access AFP assets, information and facilities in accordance with AFP and Australian Government requirements.

This guideline observes obligations under the:

- [Australian Government Protective Security Policy Framework](#)
- [AFP Commissioner's Order on Security \(Commissioner's Order 9\)](#).

5. Policy

All clearance subjects, where determined by the relevant delegate and agreed to by Coordinator Personnel Security Vetting (CPSV), must:

- hold and maintain an Australian Government security clearance, at the minimum security clearance level required in order to access AFP assets, information and facilities per s. 7 of the [AFP Commissioner's Order on Security \(CO9\)](#).
- comply with all reasonable and relevant requests from Personnel Security Vetting (PSV) for all vetting processes and procedures.

Failure to comply with this guideline may result in a security clearance review, and consequently a variation, cancellation or denial of a security clearance.

Failure to maintain a valid security clearance may result in termination of employment.

Part A – Security clearance

6. Designated Security Assessment Position (DSAP) register

Every position in the AFP employment framework is a DSAP and requires a security clearance based on the highest classification of information or assets that may be accessed.

AFP Security must maintain and review the AFP DSAP register:

- annually, as a minimum requirement
- periodically, when:
 - a position becomes vacant and before it is advertised or filled
 - the existing occupant's security clearance is revalidated.

As part of the periodic and annual DSAP reviews, National Managers must:

- review their existing DSAP requirements
- notify [CPSV](#) in writing, of any amendments to the DSAPs in their area of responsibility.

National Managers may request an amendment to the DSAP at any time. Amendments must be in writing to [CPSV](#) outlining the reasons for the change. If supported, PSV must update the DSAP register and notify the National Manager of the endorsed amendments. Where a request is not supported CPSV must notify the National Manager accordingly.

7. Security clearance levels

A delegate under [AFP Commissioner's Order on Security \(CO9\)](#) may grant AFP security clearances.

Security clearances granted by the AFP are valid, from the date of granting. Clearance subjects must submit a completed [revalidation pack](#) to [PSV](#) at least **three months** before their security clearance is due to expire.

Clearance level	Access to classified assets and information	Validity Period	Comments
Baseline	Up to and including PROTECTED	15 years	Provides access to AFPNet
Negative Vetting Level 1 (NV1)	Up to and including SECRET	10 years	AFP default level
Negative Vetting Level 2 (NV2)	Up to and including TOP SECRET Relevant compartment briefings required for access to caveat and code word information.	5 years	Mandatory interview
Positive Vetting (PV)	Access to all classification levels Relevant compartment briefings required for access to caveat, compartmented and code word information.	7 years	Annual security appraisals

For further information on the classification of assets and information to which these four security clearance levels relate, see the:

- [Access and storage requirements for information and assets](#)
- [Australian Government Protective Security Policy Framework \(PSPF\)](#).

Former security clearances of Top Secret, Secret, Highly Protected, Protected and Confidential are no longer issued. Existing AFP clearances will be recognised until whichever of the following occurs first:

- **revalidation:** the sponsor must decide the clearance level required in accordance with the DSAP register
- **change of role or duties:** the clearance subject requires access to different levels of classified AFP assets, information or facilities.

7.1 Validity periods for other access

Short-term higher access (per s. 14.1) is valid for a period specified by the CPSV and for a maximum of 3 months in 1 calendar year.

Where there is a requirement to obtain access beyond this timeframe, the clearance subject must submit a completed [Security Clearance Vetting Pack](#) and be granted a security clearance, or provisional access per s. 14.

Provisional clearance (per s. 14.2) is valid until the full security clearance is granted.

Certificate of Suitability (CoS) (per s. 20) is valid for a maximum of 24 months from the date of granting, or until the clearance subject's home agency clearance expires, whichever is sooner.

Citizenship waiver (per s. 18) is valid for 12 months from the date of granting.

8. Requirements when engaging personnel

In accordance with the [Australian Government Protective Security Policy Framework – PERSEC 1](#), AFP appointees responsible for engaging personnel, or managing or entering into contracts for the supply of services to the AFP, must ensure clearance subjects who require ongoing access to AFP assets, information and facilities:

- are eligible to have access
- have had their identity established
- are suitable to have access
- comply with:
 - Australian Government and AFP standards, protocols, guidelines and governance that safeguard the agency's resources from harm
 - the AFP Core Values detailed in the [AFP Commissioner's Order on Professional Standards \(CO2\)](#); and
 - the [AFP Character Guidelines](#) detailed in the [AFP Commissioner's Order on Security \(CO9\)](#).

For further information on security clearance requirements for accessing AFP facilities and classified information, refer to the [Access and storage requirements for information and assets](#).

9. Roles and responsibilities

9.1 Clearance subjects

All clearance subjects must:

- hold and maintain a valid AFP or AFP-recognised security clearance at the level required for their position as determined by the AFP DSAP register and the [AFP Commissioner's Order on Security \(CO9\)](#). **NB:** clearance subjects may access the level and expiry date of their individual security clearance (except for PV) via [Insight!](#) on the AFP Hub.
- ensure documentation is submitted to PSV within the required timeframes
- report all change of circumstances to [PSV](#), per s. 10 below
- comply with the AFP [Security Governance Framework](#).

Failure to comply with the AFP vetting process and/or the documented timeframes constitutes a failure to meet security obligations and may result in:

- suspension of a clearance process
- cancellation or denial of a clearance process
- review of an existing security clearance.

9.2. AFP appointees

All AFP appointees must complete annual security refresher training and make a record in their Performance Development Agreement or Charter of Performance.

AFP 'Top Secret control officers and classified document register supervising members' must undertake annual refresher training with the [AFP Communications Intelligence Security Officer](#) Team.

9.3 AFP appointees responsible for supervision or engagement of a clearance subject

All AFP appointees who supervise or are responsible for the engagement of a clearance subject must ensure:

- the clearance subject has a valid AFP or AFP-recognised security clearance at the appropriate level required for the proposed position, prior to endorsing:
 - [unescorted access to AFP facilities](#)
 - applications for [AFP ICT system access](#)
 - access to [AFP assets or information](#).
- the clearance subject has the specific compartment briefings required to perform the role
- their staff maintain an active security clearance until their separation from the AFP (supervisors may access the level and expiry date of individual security clearances via [Insight!](#) on the AFP Hub)
- the clearance subject completes all mandatory training within the AFP's stipulated timeframes, for:
 - AFP appointees this includes, but is not limited to the mandatory:
 - AFP staff induction course within 3 months of commencement
 - AFP online training courses in accordance with the Performance Development Agreement (PDA) cycle, unless otherwise specified.
 - non-appointee contractors this includes, but is not limited to, requirements detailed within:
 - the contract and/or deed of confidentiality documentation
 - legislation and Commonwealth policies, including but not limited to the:
 - [Australian Federal Police Act 1979](#) (Cth)
 - [Privacy Act 1988](#) (Cth)
 - [Public Interest Disclosure Act 2013](#) (Cth)
 - [Work Health and Safety Act 2011](#) (Cth)
 - [Australian Government Protective Security Policy Framework](#)
 - [Information Security Manual](#).

- the clearance subject is aware of and complies with (where applicable) the access conditions to information systems and AFP facilities detailed in:
 - [AFP Commissioner's Order on Security \(CO9\)](#).
 - [AFP National Guideline on information security](#).
 - AFP National Guideline on physical security (drafting)
- a report has been submitted, if they are aware a clearance subject has:
 - a reportable change of circumstance, per s. 10 below
 - been involved in a security incident, per s. 26 below.
- conduct biannual health checks with their staff. The [Security Check Appraisal Form](#) may be used to assist with discussions. Where an unreported change or a security concern is identified, supervisors must submit the completed [Security Check Appraisal Form](#) to [PSV](#) as soon as practicable.

Where a supervisor believes the clearance subject is no longer suitable to hold or maintain a security clearance, they must submit a minute to [CPSV](#) requesting a formal review.

9.4 Sponsors

All security clearance requests must be sponsored prior to PSV commencing the vetting process.

Baseline, Negative Vetting 1 and Negative Vetting 2 clearances must be sponsored by a supervisor or above from the clearance subject's business area.

Positive Vetting clearances must be sponsored by a National Manager or above and the request approved by Manager Security (Chief Security Officer).

The sponsor acts as a conduit between the clearance subject and PSV, and must ensure:

- for bulk recruitment, PSV is consulted during the planning phase
- the clearance subject is eligible, per the [Australian Government Protective Security Policy Framework \(PSPF\) PERSEC 1](#) and s. 8 above
- the level of security clearance requested is in accordance with the DSAP register which is informed by the level of exposure to AFP assets, information and facilities, as per the:
 - [AFP Commissioner's Order on Security \(Commissioner's Order 9\)](#),
 - [AFP National Guideline on information security](#).
 - AFP National Guideline on physical security (drafting)
 - [Access and storage requirements for information and assets](#)
- the clearance subject is provided with the appropriate security clearance documentation
- the 'Security Clearance Request' page, which forms part of all packs, is completed and signed.

9.5 Personnel Security Vetting (PSV)

PSV is responsible for facilitating the below clearance processes in accordance with AFP and [PSPF](#) – PERSEC requirements:

- initial
- revalidation
- upgrade/downgrade
- review for cause
- recognition and transfer of other Australian Government security clearances
- certificate of suitability (COS)
- clearance maintenance (aftercare).

The above processes may result in any of the following clearance outcomes:

- grant
- conditional grant (eligible and suitable to hold a clearance with conditions or aftercare requirements)
- continue
- vary (upgrade, downgrade, conditional)
- deny (subject to procedural fairness, per s. 11.6 below)
- cancel (sponsorship removed, clearance requirement not confirmed, non-compliance).

PSV assessment officer

PSV assessment officers must ensure:

- clearance subjects are Australian citizens or have been issued a citizenship waiver
- all required vetting checks and assessments are conducted as outlined in the [PSPF](#), Sensitive Material Security Management Protocol (SMSMP) and PSV Standard Operating Procedures
- integrity assessments are conducted on clearance subjects who were previously employed by or contracted to another police force or government agency (whether foreign or Australian)
- any conflict of interest is declared prior to commencing an assessment of a vetting pack, as per the [AFP National Guideline on conflicts of interest](#). Where a conflict of interest is identified, the PSV assessment officer must exclude themselves from the process, unless accepted by the PSV assessment officer's supervisor.

10. Reporting requirements

A security clearance provides a snapshot of the subject at the time their clearance is granted. Ongoing security clearance maintenance is mandatory and clearance subjects must report any [change of circumstances](#) to [Personnel Security Vetting \(PSV\)](#) as soon as practicable. Change of circumstances include, but are not limited to:

- entering into, or ceasing, a marriage or relationship
- change of name/identity (gender)
- change of address
- serious medical conditions or mental health disorders – report via a [change of health notification form](#)
- illegal drug or illicit substance usage
- alcohol and/or drug abuse
- new cohabitants (18 years and over)
- changes in financial circumstances (e.g. plus or minus \$10,000 in each instance, bankruptcy)
- ongoing contact with foreign associations
- residence or intended residence in, or visits to, foreign countries
- relatives residing in foreign countries
- changes and intended changes in citizenship or nationality
- involvement in criminal activity
- being served with a diversionary conference/restorative justice notice, by any law enforcement body, to attend education, assessment and treatment or counselling relating to any matter (where there has been no arrest or charge)
- being a witness or having an involvement in a civil or criminal matter which is not part of an AFP appointee's official duties
- being detained, arrested, charged, summonsed or the subject of an investigation in relation to a criminal matter
- attending a location where people are suspected to be engaged in criminal activity, including 'social' use of illicit substances
- involvement or associations with any individual, group, society or organisation, as detailed in the [AFP National Guideline on conflicts of interest](#)
- undertaking secondary employment
- disciplinary procedures (related to minor or serious misconduct) – refer to the [AFP Commissioner's Order on Professional Standards \(CO2\)](#).

- suspicious contact (NB: any suspicious contact from a foreign national must be reported to the Australian Security Intelligence Organisation (ASIO), as per the Australian Government Contact Reporting Scheme. Upon reporting the contact to PSV via a [change of circumstances form](#), PSV must on-forward the report to ASIO.)
- security incidents, per s. 26 below
- other significant changes in circumstances, such as major change in religious faith, political ideology or other life changes.

Any change of circumstance must be assessed by PSV and may result in:

- the retention of the information on the clearance subject's personal security file with no further action
- a request for further details
- a security investigation
- a referral to Professional Standards
- a review for cause of the security clearance
- any other action deemed necessary by PSV based on the information received.

Any queries relating to [change of circumstances](#) must be forwarded to [PSV](#).

10.1. Management reporting obligations

Clearance subjects must inform:

- their line manager
- AFP Security via a [change of circumstances form](#)
- Medical Services via a [change of health notification form](#)

where they have been:

- diagnosed with a serious medical or mental health condition which may prevent them from undertaking their normal duties
- on any medication which may affect their decision making capabilities.

Clearance subjects served with a court order must inform their line manager and Security via a [change of circumstances form](#).

Subject to any court orders or medical documentation, the line manager must decide whether to:

- request revocation or suspension of any AFP operational safety qualification, per the [AFP Commissioner's Order on Operational Safety \(CO3\)](#)
- request the removal of access to any controlled items
- request limited or the removal of access to AFP facilities
- withdraw any authorisation to drive official AFP vehicles.

The supervisor or line manager may seek advice from AFP Security through [Security Reporting and Referrals](#) on what actions may be taken, and must notify the individual of the outcome. Procedural fairness and natural justice obligations must be observed prior to taking some of the actions identified above. Supervisors or line managers should contact [AFP Legal](#) for assistance, particularly where any action may result in AFP personnel being unable to perform their normal duties.

11. Vetting outcomes

A delegate under the [AFP Commissioner's Order on Security \(CO9\)](#) may grant, deny, cancel, review or vary a security clearance.

Where a recommendation to deny, cancel or vary a security clearance is made, procedural fairness actions must be followed, per s. 11.6 below.

11.1 Grant (eligible and suitable to hold a security clearance)

A security clearance must only be granted where the clearance subject is eligible and suitable to hold a security clearance at the level required.

Clearance maintenance arrangements may be required due to the identification of possible or established integrity or security concerns, per s. 12 below.

11.2 Deny (ineligible to hold a clearance)

A security clearance may be denied where an assessment conducted by PSV identifies that a clearance subject is not eligible to hold a security clearance.

Where CPSV recommends denying a security clearance of an AFP appointee, an internal review of the process must be completed by an independent reviewer (AFP Coordinator or above from outside the Security portfolio). Upon assessing all available information, the independent reviewer must make a recommendation to the delegate under [CO9](#), on whether the security clearance should be denied.

Where a security clearance is denied, the delegate under [CO9](#) must:

- document their decision in the relevant security vetting file
- notify the ASIO per the [PSPF – Australian Government Personnel Security Protocol](#).

11.3 Cancel

A security clearance may be cancelled by withdrawal or de-activation:

- at the request of the sponsor
- where the sponsorship or clearance requirement cannot be confirmed
- where a clearance subject has been assessed by PSV to be non-compliant.

Where a security clearance is cancelled by the:

- sponsor – the sponsor must provide written advice to [PSV](#) outlining the reasons for the cancellation
- delegate under [Attachment 1](#) to the [CO9](#) – the delegate must formally document their decision (and include on the clearance subjects personnel security file) for the cancellation.

11.4 Vary (upgrade, downgrade or conditional)

A security clearance may be varied where a clearance subject:

- holds or transfers to a position which requires a different security clearance level
- is assessed by PSV as ineligible or unsuitable to maintain a security clearance at the level held
- is assessed by PSV as being eligible and suitable to hold a security clearance with conditions and/or maintenance requirements.

11.5 Review for cause

A review for cause may be required where an integrity or security concern arises about a clearance subject.

PSV must undertake any checks required to resolve the concern(s) that led to the initiation of the review for cause. This may include:

- targeted checks
- formal direction to provide documents or participate in an interview
- a full review of the security clearance in question.

Where a clearance subject is directed to participate in an interview, they must ensure all accoutrements are stored in a gun locker prior to attending the interview.

Upon completion of a review for cause, a clearance may be cancelled, denied, varied or continued.

11.6 Procedural fairness (post review)

Where information obtained in an assessment process by PSV indicates a clearance subject may be ineligible or unsuitable to hold a security clearance (including maintaining an existing security clearance) and a recommendation to deny, cancel or vary the security clearance is made, the clearance subject must be advised in writing.

Where possible, the clearance subject should be advised of the reasons for the denial, cancellation or variation to their clearance. Some reasons may be withheld dependent on:

- the nature of the information
- the circumstances in which the information was received
- any relevant operational or privilege considerations.

The clearance subject has 14 days from receipt of the notification to show cause (respond) in writing to the CPSV outlining why the security clearance should not be denied, cancelled or varied. The response must be assessed against the initial grounds for the denial, cancellation or variation.

Where the clearance subject fails to respond within 14 days, their security clearance may be automatically suspended, denied or varied.

A final decision on a clearance subject's suitability to hold a security clearance or level of clearance must be communicated in writing to the clearance subject by the relevant delegate under the [CO9](#). This should occur within 28 days of receipt of the clearance subject's written submission.

11.7 Review or appeal of a clearance decision

Internal review

The avenues for review vary depending on whether the clearance subject is already employed by the AFP or is a prospective employee.

Where a decision has been reached by CPSV to deny an external clearance subject, they may appeal the decision by requesting an internal review in writing within 14 days of being informed.

Where CPSV recommends the denial or cancellation of a security clearance, an internal review of the process and recommendation will commence automatically.

Upon completion of the internal review, the delegate under [CO9](#) for cancelling or varying a security clearance of an internal clearance subject, must review all available information and make a final decision on the recommended denial. The [CO9](#) delegate must inform the clearance subject of the outcome in accordance with the [PSPF – personnel security guidelines vetting practices](#).

Appeal

Clearance subjects unsatisfied with the internal review process may request a review of the process through the:

- [Commonwealth Ombudsman](#)
- Federal Court or High Court of Australia
- Administrative Appeals Tribunal against any assessment or decision made as a result of the ASIO assessment.

Clearance subjects may also lodge a formal complaint to the:

- Privacy Commissioner, if they feel that there was a breach of the [Privacy Act 1988](#) (Cth) in the way information was handled
- Human Rights Commissioner, if they feel that they have been unfairly discriminated against.

12. Clearance maintenance

Security clearances may be granted subject to specific conditions or requirements known as clearance maintenance. Additional conditions or requirements may be placed against a security clearance for the purposes of assessing a clearance subject's ongoing suitability to hold a clearance.

In accordance with [CO9](#), clearance maintenance arrangements may arise as part of the security clearance assessment, as a result of a change of circumstance, a breach or suspected breach of:

- the [employment character traits](#) (honesty, trustworthiness, maturity, tolerance, resilience and loyalty, as per s. 8 of [CO9](#))
- the [AFP Security Governance Framework](#)
- the [AFP Commissioner's Order on Professional Standards \(CO2\)](#)
- a legal contract or deed of obligation.

Clearance maintenance arrangements may include, but are not limited to:

- restrictions on access to information, facilities and/or classified resources
- additional reporting requirements, such as change of circumstances in addition to those detailed in s. 10
- formal PSV assessment processes, such as revalidation or review for cause.

Where clearance maintenance arrangements are placed against a security clearance:

- PSV must ensure all clearance maintenance arrangements are maintained
- clearance subjects must ensure they comply with all clearance maintenance arrangements.

Clearance subjects must comply with all reasonable and relevant requests for information from PSV to maintain their security clearance.

Where a security clearance is under review by PSV as a result of an identified integrity issue, the Commissioner or their delegate may, until the review is finalised:

- suspend the clearance subject from performing duties for the AFP, per Part 2, Division 1 of the [Australian Federal Police Regulations 2018](#) (Cth)
- assign the clearance subject to other duties, per s. 40TD of the [Australian Federal Police Act 1979](#) (Cth).

PSV's assessment may result in a permanent or temporary downgrade, or removal of a security clearance.

In accordance with the [PSPF](#), PSV may brief the clearance subject's supervisor of the clearance maintenance arrangements where there is a need for closer workplace supervision.

13. Personal information

All information collected as part of the security clearance process is considered sensitive and must be secured in accordance with the:

- security protocols under the Protective Security Policy Framework
- [Australian Privacy Principles](#) for personal information
- [AFP National Guideline on privacy](#).

13.1 Recording of interviews

Where an interview is conducted as part of any security clearance process, it must be digitally recorded.

All digital recordings must be retained on the clearance subject's personal security file, in CD/DVD format, and must not be retained in an ICT system. This information is only accessible by AFP appointees from Security and Professional Standards with written approval from CPSV.

13.2 Disposal of security vetting files

All security vetting files are a Commonwealth record for the purposes of the [Archives Act 1983](#) (Cth). Security vetting files must be retained for a minimum of 5 years after a clearance subject's separation from the AFP, as per the [Archives Act 1983](#) (Cth) and the [Administrative Functions Disposal Authority](#).

Part B – Form of access

14. Temporary access

Temporary access must only be granted by a delegate under the [CO9](#) after risks to the AFP and the Commonwealth have been assessed.

The temporary access process must not be used to expedite recruitment where workforce planning may have avoided such a requirement.

Temporary access provisions must:

- only be granted in exceptional circumstances
- not be used for access to information, facilities or assets classified Top Secret
- not be used to grant access to caveat, compartmented or code word information
- not be applied to positions where security clearances are used only as a measure of assurance, where there is no access to classified information.

When an individual is granted temporary access, sponsors must ensure the individual:

- only accesses information, assets and facilities essential to their duties with the AFP
- is provided with a security briefing
- where required, signs an undertaking to protect information that may be accessed.

Types of temporary access include short-term access and provisional access.

14.1. Short-term higher access

Short-term higher access allows access to information, assets and facilities when an individual:

- does not hold a security clearance at the appropriate level
- is not being assessed for a security clearance
- is yet to submit a completed security clearance pack.

Short-term higher access:

- to **TOP SECRET** material is only available, in exceptional circumstances, to individuals who hold an NV1 clearance
- to **PROTECTED** material must only be granted where there is an exceptional business need for access
- must only be granted where the:
 - exception is critical to the AFP meeting its outcomes
 - risks can be mitigated or managed.

- must be assessed in accordance with the [Australian Government Protective Security Policy Framework \(PSPF\)](#).
- must only be granted for a cumulative maximum of three months per calendar year.

To grant a request for short-term higher access, the delegate under [CO9](#) must be in receipt of a:

- brief outlining the critical AFP business need for a person who has not been security cleared
- risk assessment ensuring all foreseeable risks have been comprehensively assessed and treated in accordance with the [AFP National Guideline on risk management](#).

The delegate under [CO9](#) may change the type of access granted to an individual from short-term to provisional, where PSV confirm a completed pack has been received and there are no indicators that it will be a complex process.

14.2. Provisional clearances

Clearance subjects undertaking an NV1 clearance process may be granted provisional access where:

- PSV has not identified any adverse information in the initial assessment of the clearance documentation
- the clearance subject's criminal history, background checks and integrity assessments are returned with no adverse issues identified.

To grant a request for other provisional access, the delegate under [CO9](#) must be satisfied:

- there are no indicators suggesting the security clearance may be a complex process
- the clearance subject's general suitability for a security clearance is not in question by PSV
- all background checks, except those undertaken by the ASIO and external agency integrity or professional standards units, have been received and assessed
- if the clearance subject holds, or has held, an Australian government security clearance with another agency, the personnel security file of that agency has been transferred and reviewed by PSV.

Where a provisional clearance is granted, the following conditions must be applied:

- the clearance is granted for the purpose of early engagement with the AFP, it is **not** a complete security clearance
- the provisional access is **not** a guarantee that a full clearance will be granted
- access to material classified above **PROTECTED** is **not** allowed
- the clearance will continue to be processed, with the clearance sponsor (and the clearance subject if an existing employee) notified when a full clearance is granted
- the clearance subject must be notified of their provisional clearance and agree to these conditions
- the clearance subject must be advised that their engagement may be terminated should they not be found suitable for the full grant of a security clearance.

Where a clearance subject with provisional access is found not suitable to hold a full security clearance at the required level, their engagement with the AFP must be terminated as soon as practicable.

15. Uncheckable background

For an individual to be eligible for an Australian Government security clearance, background checks must be undertaken in Australia. It is expected that individuals undergoing an AFP security clearance will have strong established ties to Australia.

Any clearance subject who has spent greater than 12 months (accumulative) out of Australia is considered to have an uncheckable background. PSV may request additional information from the clearance subject to establish an adequate level of assurance about their life and background. Where the clearance subject is unable to provide sufficient or supportive information regarding their background, it may not be possible to continue with the clearance assessment.

16. Foreign nationals

Sponsors must demonstrate an exceptional business need for a foreign national to access AFP assets, information and facilities. A foreign national must not be granted a certificate of suitability or security clearance without first being granted a citizenship waiver per s. 18 below.

Where an external agreement with a foreign government includes details of recognition of clearances, the embedded exchange officers do not need a Commonwealth security clearance. The recognition of clearances is only for officers who are embedded as part of the agreement with the foreign government; these arrangements must not be used for other people of the same nationality who are employed by the AFP.

To seek access to AFP assets, information and facilities, a foreign national must:

- where they are from the United States of America, United Kingdom, New Zealand or Canada, and hold a valid security clearance in that country, complete the [Certificate of Suitability pack](#)
- provide evidence of any foreign security clearance.

The sponsor must provide PSV:

- the citizenship waiver for engagement
- in cases where the foreign national has an uncheckable background, a Commissioner's waiver per s. 19 below
- a risk assessment in accordance with the [AFP National Guideline on risk management](#), assessing the proposed access
- a minute addressed to the CPSV, detailing:
 - the need to engage the foreign national
 - their proposed role
 - access requirements
 - the expected length of the engagement.

PSV must undertake an assessment, based on all available information before:

- making a determination of the clearance subject's suitability for access to AFP assets and/or information
- advising the sponsor of the outcome.

Sponsors must apply the need-to-know principle regarding access to assets, information and facilities by the foreign national, and notify all staff that may have contact with them. Foreign nationals must not be given access to material containing a caveat per the [Protective Security Policy Framework \(PSPF\)](#).

AFP appointees must comply with any treaties governing the disclosure of information to security-cleared foreign nationals. To resolve doubt over whether an agreement exists, AFP appointees must seek advice from the Department of Foreign Affairs and Trade (DFAT). Regardless of any agreement, AFP appointees must not disclose to a foreign national (even if security cleared) any information marked with a restriction, including but not limited to:

- the caveat 'AUSTEO', 'AGAO', or Australian COMSEC information (information marked with caveats 'Releasable to' or 'Eyes Only' must only be disseminated to or accessed by foreign nationals who are listed in the marking, per the [Security Caveat Guidelines](#)).
- specifically restricted as third country sourced.

Sponsors must notify PSV prior to any role change or employment extension past the original period to have the waiver re-assessed. As waivers are only valid for 12 months, sponsors should commence a re-assessment process at least 12 weeks prior to the expiry of the waiver.

17. Locally engaged staff (LES)

All LES requiring access to AFP assets, information and facilities must hold an AFP or AFP-recognised security clearance. Sponsors must ensure the level of security clearance required is determined by a risk assessment completed in accordance with the [AFP National Guideline on risk management](#).

If the requesting area operates within a DFAT facility, and the LES are employed by DFAT, then DFAT are responsible for conducting security clearance assessments, unless they advise otherwise in writing. For all other locations outside DFAT's control, the AFP must conduct the security clearance assessment process to the [Protective Security Policy Framework \(PSPF\)](#) standard.

Once DFAT grant a security clearance, the AFP sponsor must submit a completed [AFP certificate of suitability](#) pack (through International-Network, via the International Diplomatic Mail Bag) for approval by the Manager International Engagement prior to submitting to PSV.

18. Citizenship waiver

A delegate identified in Attachment 1 to the [CO9](#) may waive citizenship requirements for the purposes of a security clearance.

Citizenship waivers must only be granted where it can be demonstrated the:

- foreign national possesses a relevant skill set not available from an Australian citizen
- role cannot be performed by an Australian citizen
- there is no conflict of interest in relation to the person's country of allegiance or the role being undertaken
- foreign national is a permanent resident and is actively seeking citizenship, and the process will be concluded in a reasonable period
- foreign national is a subject matter expert required to provide training, advice or support to the AFP for a short period.

In all cases advice must be sought from PSV before a process for a non-citizen is commenced.

After reviewing a current threat assessment for the particular country, the sponsor requesting the waiver must submit a:

- minute to the CPSV detailing the need to engage a non-citizen over an Australian citizen, including a proposed end date to the requirement
- risk assessment ensuring all foreseeable risks associated with engaging the non-citizen have been comprehensively assessed and treated in accordance with the [AFP National Guideline on risk management](#).

CPSV must submit a minute to the Manager Security (Chief Security Officer) with:

- the sponsor's submission
- recommendations that may include specific conditions to the waiver
- any additional relevant information regarding the applicant's background or suitability.

Manager Security (Chief Security Officer) must return the waiver whether approved or denied to CPSV, who must arrange the appropriate clearance action and ensure the waiver is attached to the foreign national's personal security file.

The granting of a citizenship waiver does not:

- guarantee or replace granting a security clearance
- permit non-Australian citizens to access information containing a caveat, as per s. 16 above.

Clearance subjects requiring citizenship waivers are subject to the same security reporting requirements per s. 10 above.

Citizenship waivers are only valid for 12 months and must be renewed following the same process as the initial application. Renewals should be commenced at least 12 weeks prior to the waiver's expiry date to allow time for the process to be completed. Late submissions may impact the clearance subject's access to AFP assets, information and facilities until the waiver is renewed.

The appropriate security vetting pack will be issued to the requesting business area once waiver approval has been received. In each instance PSV must be contacted for advice.

19. Commissioner's waiver

A Commissioner's waiver allows individuals to gain a security clearance, who would not otherwise be eligible.

A delegate identified in Attachment 1 to [CO9](#) may waive eligibility requirements for the purposes of a security clearance.

Where a citizenship waiver has been granted for an individual per s. 18 above, the delegate to grant a Commissioner's waiver must not be the same.

In accordance with [PERSEC 5](#), all security clearances issued with a Commissioner's waiver are:

- role specific
- time-limited
- subject to review
- not portable.

Commissioner's waivers must only be granted where it can be demonstrated that the advantage to the AFP issuing a security clearance (to allow access to information, resources or AFP facilities for a person who fails to meet the security clearance eligibility requirements) outweighs the risk involved. Circumstances may include the:

- individual is critical to the agency meeting its outcomes and the risks to the agency can be mitigated and/or managed
- role cannot be redesigned so that access to classified information or resources is restricted to existing employees with the appropriate clearance.

To request a Commissioner's waiver, the sponsor must submit to the CPSV:

- a minute justifying the need to engage an ineligible individual, including a proposed end date to the requirement (must not exceed 5 years)
- a risk assessment ensuring all foreseeable risks associated with engaging an ineligible individual have been comprehensively assessed and treated in accordance with the [AFP National Guideline on risk management](#)
- the clearance subject's agreement to meet the conditions set out in the waiver and accompanying risk assessment.

CPSV must submit a minute to Manager Security (Chief Security Officer) advising of the:

- Commissioner's waiver
- sponsor's submission
- recommendations that may include specific conditions to the waiver
- results of intelligence or integrity checks conducted.

Manager Security (Chief Security Officer) must submit the request, with comment, to the [CO9](#) delegate.

The waiver (either approved or denied) must then be returned to CPSV, who must take the appropriate action, including:

- advising the sponsor of the outcome

- recording the result in the individual's personal security file or on PROMIS.

20. Certificate of Suitability (CoS)

The CoS process may be used to recognise an existing Australian Government security clearance for individuals seconded to the AFP. Clearance for any subsequent period(s) of secondment must be subject to the CoS application and assessment by PSV.

Clearance subjects from other Commonwealth, state or territory law enforcement agencies, who hold a valid Australian Government security clearance, prior to obtaining access to AFP assets, information or facilities, must:

- undertake an AFP CoS process: complete a [CoS pack](#), ensuring the appropriate section is completed by their owning agency's security advisor
- receive approval from PSV.

Access must only be granted:

- up to the security clearance level currently held by the clearance subject
- for a period of up to 24 months
- while the clearance subject's home agency clearance is valid
- until the cessation of the secondment.

Where the existing clearance has been granted under a waiver, a separate waiver process must be undertaken by the AFP prior to providing the secondee access to AFP assets or information. Additional assessment processes may be required, including, but not limited to:

- employment suitability assessment
- organisational suitability assessment
- other assessments based on any information received by PSV.

A CoS must not be used for AFP personnel who perform ICT administrator roles.

21. Organisational suitability assessment (OSA) - contractors

The AFP may seek to engage a contractor to provide specific services. Prior to engagement, all contractors must undergo the OSA process and the information provided by those individuals will be assessed against the [AFP Character Guidelines](#). Where conflicting information is identified, the contractor will be contacted to enable an opportunity to provide a response, thereby affording procedural fairness. At the completion of the OSA process, the AFP sponsor will be notified in writing of the outcome.

Where the OSA applicant is deemed suitable, they will then be asked to submit a full security clearance vetting pack to the level required for the position. The security clearance assessment and the OSA are entirely separate processes. Success at the OSA stage does not indicate a security clearance will be granted. The additional information will be assessed in accordance with PSV protocols to determine the clearance subject's suitability to hold an AFP security clearance.

Where an OSA applicant is deemed unsuitable, the AFP sponsor will be notified accordingly and no further security assessment will be undertaken. The AFP sponsor is responsible for notifying the contractor of this outcome.

Prior to engaging a contractor or consultant, the AFP appointee must:

- consider and comply with the [AFP National Guideline on procurement and contracting](#)
- determine whether the contractor/consultant and/or their personnel should be:
 - engaged under s. 35 of the [Australian Federal Police Act 1979](#) (Cth) and deemed to be AFP appointee (refer to the [AFP Appointee \(Contractors\) Toolkit](#))
 - subjected to AFP's security clearance process

- the subject of a risk assessment.

This is particularly critical in areas such as:

- protection or development of AFP critical infrastructure
- development of AFP systems management, including ICT or other significant operations management tools
- activities requiring access to classified information or systems housing information rated at **PROTECTED** or above
- activities within the AFP's operating environment where the performance of that role will expose personnel to sensitive practice and procedural activities, sensitive facilities or information
- access to/control of AFP resources (consideration to be given to classification, value and/or quantity of assets which are the subject of the engagement)
- an increase in [AFP's Security Alert Level](#) to 3 and above.

When engaging a non-appointee contractor, the decision must be:

- informed by a risk assessment ([AFP National Guideline on risk management](#))
- informed by an OSA
- approved by the relevant delegate (for the endorsement of expenditure)
- recorded in a legal contract for contractors, or a deed of confidentiality for specified personnel of a service provider, and must include:
 - any separation requirements, per s. 24
 - [security](#), [public interest disclosure](#) and [work health and safety](#) requirements
 - a clause noting at times a security clearance may not be a suitable risk mitigation for services contracted out to external providers, therefore a requirement to engage the contractor as an AFP appointee may exist.

Consultation with [AFP Legal](#) is recommended.

22. Transfer of other Commonwealth agency clearances

PSV must only transfer a valid Australian Government security clearance from another Commonwealth agency for potential AFP appointees, in accordance with the [Australian Government Protective Security Policy Framework](#).

Prior to any offers of employment being made to a person with a valid Australian Government clearance, the normal recruitment process must be undertaken. This must include the clearance subject's completion of the employment suitability questionnaire that may be referred to Professional Standards.

When a clearance subject accepts an offer of employment they will be provided with a security clearance transfer pack by their AFP sponsor or AFP Recruitment. The completed pack must be returned to the AFP sponsor or AFP Recruitment for endorsement prior to being provided to PSV for assessment.

23. Positive vetting (PV) security clearance

To request a PV security clearance, the clearance subject's sponsor (at National Manager level or above) must submit a Security Clearance Request–PV form (contact [Security-Vetting](#) to obtain a form) to PSV.

The request form must be:

- accompanied by a minute addressed to the Manager Security (Chief Security Officer) detailing why the clearance is required
- signed by an AFP manager or sponsor, or one rank higher in the case of executive staff (SES)
- submitted to PSV by hand, or electronically to [Security-Vetting](#).

Prior to supporting a clearance subject's request for a PV security clearance, PSV must confirm the position held by the clearance subject is recorded on the DSAP register.

PV clearance holders are required to undergo annual appraisals and a full re-validation 7 years after the date of granting. These processes will be initiated by the Australian Government Security Vetting Agency or by PSV.

24. Separations

Clearance subjects, or those granted access to AFP assets, information and facilities under other provisions outlined within Part B of this guideline, separating from the AFP, must submit a completed [Separation Acquittal Form](#) (AFP Hub) as per the [AFP National Guideline on separation](#).

Payroll Services must advise Security of all separations from the AFP by emailing [Security-Vetting](#) and [Access-Control](#) within 12 hours of receiving notification, to allow for facility and ICT system access to be removed and the security clearance made inactive.

Part C – Security Reporting

This part outlines the obligations of AFP personnel for reporting:

- security incidents
- international travel.

25. Security reporting requirements

AFP personnel must report to AFP Security in accordance with this guideline as soon as practicable after they become aware of a reportable event or circumstance.

Situations where AFP personnel must report to AFP Security include, but are not limited to:

- a breach of security, by themselves or any other individual employed by or contracted to the AFP
- suspicious activity which may cause a security incident in or around AFP premises
- any harm or threats to cause harm to an AFP appointee arising from their employment with the AFP
- undertaking any overseas travel (official or personal)
- other situations where an individual's ability to maintain a security clearance may be called into question - [change of circumstances form](#) per s. 10 above.

Information in a security incident report may be of a sensitive nature. AFP personnel should not disseminate the details of the issue beyond their supervisor, Professional Standards or AFP Security, without lawful authority. AFP Security may liaise with other portfolios within the AFP to determine what action should be taken.

AFP personnel must, where appropriate, advise their supervisor of the information being reported. It must be noted on the [security incident report](#) or [change of circumstances form](#) per s. 10, if the supervisor has been advised of the information.

AFP personnel must apply a 'common sense' approach to submitting multiple reports in situations where contact or an event is ongoing. A reporting agreement may be arranged through consultation with [AFP Security](#).

The [AFP National Guideline on the Confidant Network](#) details the support process available to all AFP appointees who have reported, or are considering reporting a breach of security.

25.1. Reporting other AFP personnel

AFP personnel must complete a [security incident report](#) if they suspect other AFP personnel of breaching security or not reporting a change in their personal circumstances. That is, if they suspect other AFP personnel of not reporting or declaring:

- involvement in criminal activity
- a breach of security
- loss of controlled items or AFP credentials
- an integrity issue that may affect an individual's suitability to hold an AFP security clearance.

There is also a requirement to report any dealings with other AFP personnel in the course of AFP duties which may be or suspected to be a security incident, particularly where that person is a suspect in a criminal investigation. This must be reported to AFP Security via a [change of circumstances form](#) per s. 10, and Professional Standards via an [integrity report](#) per the [AFP National Guideline on integrity reporting](#).

25.2. Professional Standards (PRS) reporting

In addition to the reporting requirements detailed in the [CO2](#) and the [AFP National Guideline on integrity reporting](#), AFP conduct or practices issues that involve a security issue (i.e. security incident or a change of circumstances) must be reported to AFP Security.

AFP personnel with doubts over whether an issue should be reported as a security or an integrity issue should seek advice through [Security](#) or [PRS](#) to prevent duplicate reporting.

Where PRS identify a security issue not previously reported to AFP Security, PRS must refer the matter to [Security](#).

Security must also refer matters to PRS if AFP Security identifies a conduct or practices issue:

- requiring formal referral
- not previously reported to PRS.

AFP Security may:

- seek further details from the person who reported the matter
- take further steps to manage or resolve any identified security incident or conflict of interest
- where it is identified that further assessment or action is required, consult with the relevant supervisor.

26. Security incident reporting

A security incident is any incident that could impact on the security of the AFP's people, assets, operations, information or reputation. This includes the identification of potential threats, vulnerabilities or risks directly or indirectly to the organisation, or any other occurrence that may result in negative consequences for the AFP or the Australian Government.

AFP personnel must report all security incidents by completing and submitting a [security incident report](#) (SIR).

A detailed list of AFP security incidents is located on the [SIR](#) Hub page.

Security incidents are categorised as follows:

- **Threats and harm to AFP appointees (BULWARK)** – s 47E(c)

s 47E(c)

- **Cyber security incidents** – must be initially reported by telephone to the Security Reporting and Referrals Hotline (ph: s 22(1)(a)(ii) or s 22(1)(a)(i)). A completed [SIR](#) must be submitted as soon as

practicable after the initial report, and the AFP Information Technology Security Advisor must ensure that the Manager Security (Chief Security Officer) is made aware of all cyber security incidents before reporting to other government agencies.

- **Security infringement, breach and violation** – an [SIR](#) must be submitted as soon as practicable after identifying a security infringement, breach or violation. AFP personnel who cannot initially forward a written report must telephone Security Reporting and Referrals (ph: [s 22\(1\)\(a\)\(ii\)](#) or [s 22\(1\)\(a\)\(ii\)](#)) and at the first opportunity submit a completed [SIR](#).
- **Lost or damaged AFP credentials** – must be reported via an [SIR](#) as soon as practicable after the loss or damage. Lost or stolen AFP credentials must also be reported to AFP Security by calling Access Control (during office hours 0800 -1600) on ph: [s 22\(1\)\(a\)\(ii\)](#) or as per after-hours reporting below. The replacement of the AFP credential is dependent on the submission of the [SIR](#). A signed [AFP Pass Acknowledgement form](#) (AFP Hub) must be submitted to Access Control prior to receiving a replacement AFP security pass, identity certificate, or warrant badge.
- **Suspicious activity** – must be initially reported by telephone to the Security Reporting and Referrals Hotline (ph: [s 22\(1\)\(a\)\(ii\)](#) or [s 22\(1\)\(a\)\(ii\)](#)) A completed [SIR](#) must be submitted as soon as practicable after the initial report. AFP Security must ensure the activity is immediately investigated and an assessment made against the [AFP Security Alert Level](#).

After-hours reporting

Security incidents occurring outside normal business hours must be reported to either the:

- Security Reporting and Referrals Hotline on ph [s 22\(1\)\(a\)\(ii\)](#)
- AFP Operations Coordination Centre (AOCC) Watchfloor Supervisor (urgent: [s 22\(1\)\(a\)\(ii\)](#) or non-urgent: [s 22\(1\)\(a\)\(ii\)](#)) who will assess whether to immediately contact the AFP Security on-call member or hold the information until the next business day.

AFP personnel reporting security incidents to AOCC must still submit an [SIR](#) as soon as practicable.

26.1 Security incident management

Security incidents are managed, assessed and investigated by AFP Security in accordance with the [CO9](#).

Without limiting immediate action taken by AFP personnel and supervisors, an incident assessment includes:

1. Initial assessment by supervisor (within the [SIR](#)).
2. Evaluation by AFP Security.
3. Incidents deemed to be a security breach must receive a full assessment by AFP Security, when deemed necessary.
4. Incidents deemed to be a security infringement or violation must be investigated as directed by the AFP Security Management Panel, in accordance with [CO9](#). Manager Security (Chief Security Officer) must ensure the outcomes of security investigations are incorporated in mandatory reporting to Australian government security agencies.
5. Incident response outcomes and any corrective action, mitigation or follow up measures must be advised and implemented as required.

Corrective actions may include one or more of the following:

- review of security clearance
- training and development action
- action taken to improve behaviour, including:
 - recording adverse findings on the individual's personal security file
 - counselling
 - a formal warning
 - adopting improvement strategies
 - structured changes to employment
 - changing or restricting access to AFP premises, information systems or assets

- reassigning duties
- a transfer of location
- increased supervision.

Manager Security (Chief Security Officer) must brief the AFP executive as required, including recommending a change to the AFP Security Alert Level, resulting from security incident assessments.

AFP Security must, where possible, provide feedback to the reporting individual(s) and their line managers to improve the AFP's security.

27. BULWARK – Threat to an AFP appointee

THE DOCUMENT IS RELEASED BY
THE AUSTRALIAN FEDERAL POLICE
UNDER THE FREEDOM OF INFORMATION ACT 1982

s 47E(c)

Page 23 redacted for the following reason:

s 47E(c)

THE DOCUMENT IS RELEASED BY
THE AUSTRALIAN FEDERAL POLICE
UNDER THE FREEDOM OF INFORMATION ACT 1982

27.7 Organisational Health Support

The receipt of a credible threat or perception of an increased security risk may place an AFP appointee and their family in a situation of increased stress and/or trauma. In such cases, AFP appointees should contact the [Organisational Health Triage](#) team to discuss their situation and available support options.

Organisational Health support services include, but are not limited to the:

- Welfare Officer Network,
- Employee Assistance Program
- Chaplaincy services.

The Welfare Officer Network provides emotional support and practical assistance for appointees affected by work or personal pressures. Contact details for a Local Welfare Officer are available from the [Welfare Officer Network](#) (AFP Hub).

Davidson Trahaire Corpsych (DTC) provides the AFP's Employee Assistance Program and offers confidential counselling services for appointees and immediate family members. DTC can be contacted on 1300 360 364.

AFP Chaplaincy services provide spiritual welfare and pastoral care to AFP appointees and immediate families and can be contacted on [s 22\(1\)\(a\)\(ii\)](#)

Further information on Organisational Health services is available on the [Wellness@Work](#) hub page.

28. International travel

AFP personnel must notify AFP Security of any official and/or personal overseas travel prior to undertaking that travel. Individuals must complete an [international travel notification](#) form and submit it to [Security Reporting and Referrals](#) at least 14 days prior to departure (where possible).

AFP appointees with compartment briefings must notify [Security Reporting and Referrals](#) at least 30 days prior to departure.

Depending on the circumstances of travel and destination, AFP personnel may receive a security briefing from AFP Security prior to departure.

29. Secondary employment

AFP personnel must receive approval per the [AFP National Guideline on secondary work or volunteering](#), prior to undertaking any secondary employment activity.

30. Classification of reports

AFP personnel must appropriately classify all report forms submitted according to their content and transmit them according to the:

- [Australian Government Protective Security Policy Framework](#)
- [AFP National Guideline on information management](#).

31. Compliance

Any breaches of this guideline must be reported to AFP Security via a [security incident report](#).

In addition to breaching the professional standards of the AFP, inappropriate departures from the provisions of this instrument may also constitute a breach of AFP's security and be dealt with under the security incident management practices, per the [AFP Commissioner's Order on Security \(Commissioner's Order 9\)](#).

32. Further advice

Queries about the content of this guideline should be referred to [Security Reporting and Referrals](#).

33. References

Legislation

- [Archives Act 1983](#) (Cth)
- [Australian Federal Police Act 1979](#) (Cth)
- [Australian Federal Police Regulations 2018](#) (Cth)
- [Ombudsman Act 1976](#) (Cth)
- [Privacy Act 1988](#) (Cth)
- [Public Interest Disclosure Act 2013](#) (Cth)
- [Work Health and Safety Act 2011](#) (Cth) .

AFP governance instruments

- [AFP Commissioner's Order on Professional Standards \(CO2\)](#)
- [AFP Commissioner's Order on Operational Safety \(CO3\)](#)
- [AFP Commissioner's Order on Security \(CO9\)](#)
- [AFP National Guideline on complaint management](#)
- [AFP National Guideline on the Confidant Network](#)
- [AFP National Guideline on conflicts of interest](#)
- [AFP National Guideline on controlled items](#)
- [AFP National Guideline on information management](#)
- [AFP National Guideline on information security](#)
- [AFP National Guideline on integrity reporting](#)
- [AFP National Guideline on physical security](#)
- [AFP National Guideline on privacy](#)
- [AFP National Guideline on procurement and contracting](#)
- [AFP National Guideline on public interest disclosure](#)
- [AFP National Guideline on risk management](#)
- [AFP National Guideline on secondary work or volunteering](#)

- [AFP National Guideline on separation.](#)

AFP forms

- [Australian Federal Police \(AFP\) Pass, Identity Certificate and Badge Conditions of Use – Acknowledgement Form](#)
- [Change of circumstances form](#)
- [Change of Health notification form](#)
- [Integrity Report](#)
- [International Travel Process](#)
- [Separation Acquittal Form](#)
- [Security Check Appraisal Form](#)
- [Security Incident Reporting](#)
- [Secondary Work or Volunteering Form.](#)

Vetting Packs

- [Certification of Suitability Form](#)
- [Security Clearance Initial \(NV1 & NV2\)](#)
- [Security Clearance Transfer Pack](#)
- [Security Clearance Revalidation \(NV1 & NV2\)](#)
- [Security Clearance Upgrade Pack](#)
- [Security Clearance Initial Baseline.](#)

Individual Vetting Forms

- [Form 2 – Security Clearance Questionnaire \(new clearance holders\)](#)
- [Form 2 – Security Clearance Questionnaire \(existing AFP clearance holders\)](#)
- [Form 3 – Personal Particulars Form](#)
- [Form 4 – Consent to Conduct a National Police Check \(Subject\)](#)
- [Form 4a – Consent to Obtain Personal Information \(Partner\)](#)
- [Form 5 – Financial Statement & Declaration NV1 & NV2](#)
- [Form 5a – Financial History Questionnaire](#)
- [Form 6 – Referees](#)
- [Form 7 – Handling AFP Information](#)
- [Form 8 – General Consent](#)
- [Form 9 – Statutory Declaration](#)
- [Form 10 – Supervisor Report.](#)

Contractors

- [AFP Appointee \(Contractors\) Toolkit.](#)
- [Contractor Security Clearance Pack – Baseline](#)
- [Contractor Security Clearance Pack – NV1/NV2](#)
- [Contractor Security Clearance Pack – Transfer](#)
- [Contractor OSA Pack.](#)

Other sources

- [Access and storage requirements for information and assets](#)
- [Administrative Functions Disposal Authority](#)
- [AFP Character Guidelines](#)
- [AFP Security Alert Level](#)
- [AFP Security Glossary of Terms](#)
- [Australian Government Personnel Security Protocol](#)
- [Australian Government Information Security Manual](#)
- [Australian Government Protective Security Policy Framework](#) (Attorney-General's Department)
- [Australian Government Personnel security guidelines Vetting Practices](#)
- [Change of circumstances](#)

- [Change of Health notification form](#)
- [Commonwealth Ombudsman](#)
- [Insight!](#) (via AFP Hub Tools and utilities)
- [Integrity Report](#)
- [International Travel Process](#)
- [Organisational Health](#)
- [Security Caveats Guidelines](#)
- [Security Committee](#)
- [Security Governance Framework](#)
- [Security homepage](#)
- [Security reporting obligations.](#)

THE DOCUMENT IS RELEASED BY
THE AUSTRALIAN FEDERAL POLICE
UNDER THE FREEDOM OF INFORMATION ACT 1982