



Security Clearances

Procedural Instruction

Document ID (PPN)	<i>SM-1550</i>
TRIM record number	<i>ADD2020/4981986</i>
BCS Function	<i>Strategic management and governance</i>
Document owner	<i>Assistant Secretary, Integrity and Professional Standards</i>
Approval date	<i>9 September 2020</i>
Document Contact	<i>Director, Personnel Security and Suitability</i> <i>securityclearances@homeaffairs.gov.au</i>

Table of Contents

1. Purpose	3
2. Scope	3
3. Procedural Instruction	4
3.1. Requirement for a minimum Baseline security clearance	4
3.2. Mandatory precondition for engagement/on-boarding	4
3.3. Process for initiating and applying for a security clearance	4
3.4. Security clearance revalidation	5
3.5. Temporary Access	6
3.6. Security clearance waivers	6
3.7. Security undertakings	6
3.8. Consequences of a failure to hold/maintain a security clearance Departmental employees	6
3.8.1 Departmental employees	7
3.8.2 Contractors and consultants	7
3.9. Review rights	7
3.9.1 Failure to maintain an essential qualification	7
3.9.2 AGSVA decision not to grant a security clearance	7
3.10. Liability for security clearance costs	7
4. Accountability and Responsibility	8
Statement of Expectation	8
5. Version Control	9
Attachment A – Definitions	10
Attachment B – Assurance and Control Matrix	11
1.1. Powers and Obligations	11
1.2. Controls and Assurance	11
Attachment C – Consultation	14
1.1. Internal Consultation	14
1.2. External Consultation	14

1. Purpose

The Department of Home Affairs (the Department) provides central strategy leadership and coordination to support the entire Home Affairs Portfolio, including the Australian Border Force (ABF), the Australian Criminal Intelligence Commission (ACIC), the Australian Federal Police (AFP), the Australian Security Intelligence Organisation (ASIO), and the Australian Transaction Reports and Analysis Centre (AUSTRAC). This ensures our efforts are coordinated and consistent in delivering outcomes for Government and the Australian community in line with Government expectations.

The Department is responsible for national security and law enforcement policy, immigration, countering terrorism policy and coordination, cyber security policy and coordination, countering foreign interference policy and coordination, security and resilience of critical infrastructure, countering violent extremism programs, aviation and maritime transport security, multicultural affairs and social cohesion, border policy, customs and trade policy, and customs and trade operations.

The Department and its staff have a broad range of powers and responsibilities as well as access to a significant amount of personal and sensitive information, which if used incorrectly could have serious consequences to the security, unity and prosperity of our nation.

The work of the Department and the information that is held by (or available to) the Department is of significant value to a range of entities who may seek to act against Australia's interests or exploit the Department's personnel to further their own interests.

Within this context, the Australian Government's Protective Security Policy Framework (PSPF) contains the controls used by the Australian Government to protect its people, information and assets. The PSPF places a range of mandatory obligations on the Department, including a requirement for the Department to ensure that all personnel who access security classified Australian Government material hold a Commonwealth security clearance at the appropriate level. Additionally, under the PSPF, agencies may use security clearances as an assurance measure in addition to their employment screening and agency specific controls where the agency risk assessment deems the security clearance process is to apply.

To operationalise this requirement within the Department, the Secretary has issued a direction under section 55 of the *Australian Border Force Act 2015* (ABF Act) (the *Secretary's Direction on Employment Suitability and Security Screening*) that requires all Immigration and Border Protection (IBP) workers to obtain and maintain a minimum Baseline security clearance (or higher, depending on the particular classified information, systems or premises that individual is required to access). In addition, Departmental security policy requires that all other individuals who require non-public access to Departmental resources must also obtain and maintain a minimum Baseline security clearance (or higher as required).

A Commonwealth security clearance (security clearance) is a determination by the Australian Government Security Vetting Agency (AGSVA) or other relevant exempt vetting agency that will allow the holder access to security classified resources.

2. Scope

This Procedural Instruction applies to all IBP workers as defined in section 4 of the *Australian Border Force Act 2015*. This term includes:

- all APS employees in the Department;
- secondees from other government agencies, foreign governments or international bodies;
- other persons authorised to be an 'officer of Customs' under the *Customs Act 1901* or an 'officer' under the *Migration Act 1958*;

- contractors and consultants, and their employees and subcontractors, who are:
 - performing services 'in-house' (that is physically located in premises that are owned, managed, controlled, leased, contracted by or operated by the Department); or
 - who are otherwise performing services that require non-public access to Department assets.

3. Procedural Instruction

3.1. Requirement for a minimum Baseline security clearance

Subject to the timing, conditions and security clearance waivers described below, all individuals who are subject to this Procedural Instruction must obtain and maintain, at a minimum, a Baseline security clearance. This Secretary has issued a direction under section 55 of the ABF Act, known as the Secretary's Direction on Employment Suitability and Security Screening which requires all IBP workers to obtain and maintain a minimum Baseline security clearance.

Positions requiring a higher level of security clearance will be determined by the relevant business area in collaboration with Integrity and Professional Standards Branch (I&PS) and in accordance with the Protective Security Policy Framework based on the highest level of security classified resources the individual is routinely required to access in order to perform their role.

A Baseline security clearance provides ongoing access to classified information and resources up to and including PROTECTED. Given the nature and risk of the business conducted by the Department, and the volume and classification of information required to be shared within the Department, a minimum Baseline security clearance for all IBP workers allow greater efficiency and interoperability.

3.2. Mandatory precondition for engagement/on-boarding

Individuals who are subject to this Procedural Instruction must hold a minimum Baseline security clearance as a precondition of their engagement and before commencement / on-boarding into the Department.

3.3. Process for initiating and applying for a security clearance

The process to initiate a security clearance for onboarding purposes is triggered through an Employment Suitability Clearance (ESC) application:

1. For APS employees, the ESC application is initiated by the Department's recruitment team.
2. For contractors, the ESC application is initiated by the contract managers.

I&PS will verify with AGSVA and/or other vetting agencies whether the individual holds a current security clearance at the required level and if applicable 'sponsor' the existing security clearance. If not, a new security clearance process will be initiated.

All requests for security clearances above Baseline will require a business case supported by the Director of the line area. Please email securityclearances@homeaffairs.gov.au to request the business case template. This will be provided to the appropriate I&PS delegate for consideration prior to Negative Vetting 1 and 2 clearances being initiated.

Positive Vetting (PV) clearances require Chief Operating Officer (COO) approval. Please email securityclearances@homeaffairs.gov.au for the PV request forms.

Once I&PS has initiated a security clearance with AGSVA, applicants will be asked by AGSVA to complete a security clearance pack comprising of:

- security clearance ePack questionnaire—*applicants will need to complete and submit this online questionnaire to AGSVA within 28 days*
- supporting documentation—*applicants will also need to:*
 1. complete a number of forms provided in the security clearance ePack
 2. provide AGSVA with personal documents to confirm their identity and background.

For more information, refer to: [AGSVA Clearance Subject - FAQ](#)

Several weeks may elapse between submitting a request form and AGSVA making contact to commence the security clearance process. Individuals must plan for this to ensure that completed security clearance ePacks are lodged within the specified time frames.

Compliance with this requirement to hold a minimum of a Baseline clearance is monitored by I&PS.

3.4. Security clearance revalidation

AGSVA is responsible for initiating and managing the revalidation and re-evaluation process. AGSVA will contact the Personnel Security Team when you are required to undergo a review.

For staff who hold a Baseline security clearance, the Personnel Security Team will confirm the ongoing requirement via AGSVA's online portal.

For staff who hold a NV1 or higher security clearance, a business case template will be sent to the clearance holder and their EL2, requesting justification as to why the higher-level clearance is required. Please note: If no response is received by the line area, AGSVA will automatically downgrade the security clearance and remove the Department's sponsorship on the clearance expiry date.

If there is no longer a requirement to hold a NV1 or higher security clearance, the clearance will be downgraded accordingly.

For more information, refer to: [AGSVA Clearance Subject - FAQ](#)

3.5. Temporary Access

Temporary (rather than ongoing access) to classified information may be required in some limited circumstances. Temporary access may be provided up to and including SECRET level information without a security clearance, after the risks of doing so have been assessed. Temporary access to TOP SECRET information requires an existing Negative Vetting 1 security clearance.

For more information, please email: securityclearances@homeaffairs.gov.au

3.6. Security clearance waivers

The Secretary of the Department, Deputy Secretary Executive, First Assistant Secretary Integrity, Security and Assurance Division and Assistant Secretary I&PS may, at their discretion, waive the requirement to hold a security clearance where an individual does not require access to security classified information or resources. However, given the volume and classification of information required to be shared within the Department and the practicalities of managing risk in this context, a waiver is not granted lightly and will be based on a risk assessment of the individual circumstances.

To seek a security clearance waiver, the relevant business area must, in consultation with I&PS, undertake a risk assessment to determine the risks associated with a person in a particular position not holding a security clearance. The risks assessment must be cleared through the First Assistant Secretary of the relevant business area and submitted to the Assistant Secretary I&PS (via securityclearances@homeaffairs.gov.au). I&PS will submit the request to the decision maker, as appropriate, for consideration and decision.

3.7. Security undertakings

A security undertaking is an internal administrative mechanism within easySAP. It must only be used while an individual is awaiting the outcome of an application to upgrade a security clearance, while they hold, at a minimum, a Baseline security clearance. Where an individual has agreed to a security undertaking in easySAP, business areas must comply with relevant policies and legislation regarding access to security classified information. *A security undertaking is not a security clearance but rather recognition that the position an individual is currently occupying usually requires a higher level of security clearance than the occupant holds and an undertaking by the occupant not to access material above the level of security clearance that they currently hold.*

A security undertaking is separate to and in no way equates to a Commonwealth security clearance.

3.8. Consequences of a failure to hold/maintain a security clearance

This Procedural Instruction does not alter the legal requirements under the relevant legislative framework. Pursuant to the *Secretary's Direction on Employment Suitability and Security Screening* of 1 July 2015, made under s55(1) of the ABF Act, IBP workers who are required to hold and maintain an Employment Suitability Clearance (ESC) must also hold and maintain, at a minimum, a Baseline security clearance.

3.8.1. Departmental employees

Failure to comply with the Secretary Directions may constitute a failure to comply with a lawful and reasonable direction and give rise to a breach of the APS Code of Conduct, resulting in the possible imposition of a sanction.

Failing to obtain or maintain a minimum Baseline security clearance at all times may lead to an assessment that the employee lacks or has lost an essential qualification for performing their duties, potentially giving rise to a ground for termination of employment pursuant to s29(3)(b) of the *Public Service Act 1999* (Public Service Act).

3.8.2. Contractors and consultants

All internal contractors and consultants (other than locally engaged staff at overseas posts) and external contractors who require non-public access to departmental assets (unless the delegate has determined otherwise) are subject to the requirement to hold and maintain a minimum Baseline security clearance.

Failure to obtain or maintain a minimum Baseline security clearance may result in the relevant contractor or consultant personnel being required to cease performing services for the Department, or the contract being terminated. Legal advice should be obtained prior to such action being taken.

Where a contract is terminated or an employee of a contracted company is removed from working for the Department for reasons that could impact their suitability to hold a security clearance, the contract manager must advise I&PS.

3.9. Review rights

3.9.1. Failure to maintain an essential qualification

Any employee who is employed under the Public Service Act and whose employment is terminated for failing to maintain an essential qualification is entitled to consider a claim for unfair dismissal under the *Fair Work Act 2009* (Cth).

Any non-Senior Executive Service (SES) employee who is employed under the Public Service Act is entitled to seek a review of action pursuant to section 33(1) of the Public Service Act whilst they are an employee.

Any individual is entitled to seek independent legal advice on other avenues of review, subject to compliance with the relevant legislative disclosure power applicable to the Department at the time.

3.9.2. AGSVA decision not to grant a security clearance

APS Employees

In the first instance, the avenue of appeal is to write to the Secretary of Defence. If you are not satisfied with the response, a secondary review can be submitted to the Merit Protection Commissioner.

Non-APS Employees and Contractors/Consultants

In the first instance, the avenue of appeal is to write to the Secretary of Defence. If you are not satisfied with the response, a complaint can be submitted to the Commonwealth Ombudsman requesting a review of the decision.

For more information, refer to: <http://www.defence.gov.au/agsva/FAQ/clearance-subject.asp>.

3.10. Liability for security clearance costs

Effective from 1 July 2019, the Department implemented a requirement for the costs associated with security clearances for Departmental contractors and consultants to be charged back to the relevant vendor, where the Department's contractual arrangements permit it to do so.

Business areas and contract managers must ensure that all new contractual arrangements include a clear and unambiguous provision for the vendor to pay for security clearances for their contractors and consultants.

4. Accountability and Responsibility

Role	Description
All individuals who are subject to this Procedural Instruction	Comply with this Procedural Instruction in accordance with the provisions specified above.
Line managers and contract managers	Ensure all personnel they manage are aware of their obligations regarding security clearances.
Integrity and Professional Standards Branch	Receiving, triaging and assessing declarable circumstances reports (and on-forwarding to AGSVA or other third parties as appropriate).
Director, Personnel Security and Suitability Section	Policy responsibility for ensuring this Procedural Instruction complies with the Department's relevant mandatory obligations under the Protective Security Policy Framework.
Division Heads (SES Band 2)	Own policy and procedure for the functions within the division and are responsible for approving policy statements for the functions owned by their division, ensuring there is high-level support for the outlined policy intent. Are accountable for ensuring the policy statement aligns with the strategic objectives of the Department.
Branch Heads (SES Band 1)	Owner and responsible for the development of policy statement documents for the functions of the branch. Approve PI for the functions owned by the branch, ensuring the policy statement owner has been consulted in the process and confirms that the procedural instruction is in line with any tiered policy statement.

Statement of Expectation

The APS Code of Conduct states that 'an APS employee must comply with any lawful and reasonable direction given by someone in the employee's Agency who has authority to give the direction' (subsection 13(5) of the Public Service Act).

Failure by an APS employee to comply with any direction contained in a PPCF document may be determined to be a breach of the APS Code of Conduct, which could result in sanctions up to and including termination of employment, as set out in subsection 15(1) of the Public Service Act.

The Secretary's Professional Standards Direction, issued under subsection 55(1) of the ABF Act, requires all IBP workers who are not APS employees (such as contractors or consultants) to comply with any lawful and reasonable direction given by someone in the Department with authority to issue that direction.

Failure by an IBP worker who is not an APS employee to comply with a direction contained in a PPCF document may be treated as a breach of the Professional Standards Direction, which may result in the termination of their engagement under section 57 of the ABF Act. Non-compliance may also be addressed under the terms of the contract engaging the contractor or consultant.

5. Version Control

Version number	Date of issue	Author(s)	Brief description of change
0.1	27/06/2019	Assistant Director, Employment Suitability Section	Initial draft of PI in new PPCF format
0.2	10/07/2020	Assistant Director, Personnel Security & Suitability	Revised draft of PI in accordance with the Department's new Operating Model 2020.
0.3	20/07/2020	Personnel Security Team	Team review

Attachment A – Definitions

Term	Acronym (if applicable)	Definition
Australian Border Force	ABF	The ABF is an operational law enforcement workforce trained and equipped to undertake functions across the border continuum.
Australian Government Security Vetting Agency	AGSVA	The Australian Government Security Vetting Agency (AGSVA) is the central agency for the processing and granting of security clearances for the majority of Australian Government agencies and state and territory agencies.
Australian Public Service	APS	Australian Public Service
Department of Home Affairs	The Department	The Department of Home Affairs, including the Australian Border Force.
Immigration and Border Protection worker	IBP worker	Defined in the Secretary's Determination of Immigration and Border Protection Workers and under subsection 4(1) of the ABF Act, includes but is not limited to: <ul style="list-style-type: none"> • all APS employees in the Department • persons employed by an Agency under the Public Service Act 1999 whose services are made available to the Department (often referred to as 'secondees') • persons engaged as consultants or contractors to perform services for the Department in-house in the Department • persons engaged as consultants or contractors to performing services for the Department that require non-public access to Departmental Assets.
Integrity and Professional Standards Branch	I&PS	Administers the Professional Standards and Integrity Frameworks, which set out the standards of integrity and ethical behaviour required by all employees of the Department.
Policy and Procedure Control Framework	PPCF	The Policy and Procedure Control Framework mandates a consistent and integrated approach to the development and management of the Department's policies and procedures. The PPCF is aligned to, and complements, the Department's Risk Management Framework, Quality Management Framework and Information Environment Strategy.
Policy Statement	PS	A statement of principle which outlines statutory, regulatory or organisational requirement in line with the strategic direction of the Department and the Australian Government.
Procedural Instruction	PI	Describes how to implement a Policy Statement by outlining actions in relation to a particular activity.

Attachment B – Assurance and Control Matrix

1.1. Powers and Obligations

Legislative Provision			Is this a delegable power?	If delegable, list the relevant instruments of delegation
Legislation	Reference (e.g. section)	Provision		
<i>Australian Border Force Act 2015</i>	55	The Secretary may give directions to IBP workers in connection with the administration and control of the Department	No	
<i>Public Service Act 1999</i>	13	Section 13 of the <i>Public Service Act</i> contains the APS Code of Conduct.	No	

1.2. Controls and Assurance

Related Policy
<ul style="list-style-type: none"> Records Management Policy (PPN TI-1094)

<p>Procedures / Supporting Materials</p>	<ul style="list-style-type: none"> • Employment Suitability Screening Procedural Instruction (PPN SM-1554) • Employment Suitability Screening Process Procedural Instruction (PPN SM-1555) • Employment Suitability Clearance Assessment Criteria Supporting Material (PPN SM-1553) • Declarable Associations Procedural Instruction (PPN SM-1551) • Security Clearances Procedural Instruction (PPN SM-1550) • Declarable Circumstances Procedural Instruction (PPN SM-1552) • Drug and Alcohol Testing Procedural Instruction (PPN SM-6177) • Mandatory reporting of Serious Misconduct, Corrupt Conduct and Criminal Activity Procedural Instruction (PPN SM-1557) • Procedures for Determining Suspected Breaches of the Code of Conduct Procedural Instruction (PPN SM-1547) • Outside Employment and Voluntary Activities Procedural Instruction • Public Interest Disclosure Procedural Instruction (PPN IIB-1548) • Use of Social Media and Other Online Services (PPN SM-1560) • Dress and Appearance Standards Procedural Instruction (PPN HR-1221) • Protective Security Policy Framework • Secretary Determination of Immigration and Border Protection Workers • Secretary Determination 1 of 2015 – Professional Standards • Secretary Determination 2 of 2015 – Employment Suitability and Security Screening • Secretary Determination 3 of 2015 – Integrity Measures
<p>Training/Certification or Accreditation</p>	<p><i>The Essentials</i> mandatory eLearning module</p>
<p>Other required job role requirements</p>	<p>Employment Suitability Clearance Baseline Security Clearance</p>
<p>Other support mechanisms (eg who can provide further assistance in relation to any aspects of this instruction)</p>	<p>Employment Suitability Team esc@homeaffairs.gov.au 1300 243 717</p>
<p>Escalation arrangements</p>	<p>Director, Pre-Employment Screening Integrity and Professional Standards Branch Integrity, Security and Assurance Division</p>

Recordkeeping (eg system based facilities to record decisions)	Electronic records to be stored in secure I&PS TRIM repository or ESC Case Management System
Control Frameworks (please refer to a specific document outlining QA or QC arrangements)	Integrity Framework
Job Vocational Framework Role	All Job Roles

Attachment C – Consultation

1.1. Internal Consultation

- Integrity, Security and Assurance Division
- Legal Group
- Media and Engagement Branch
- Procurement Policy and Improvement Branch
- all staff through Department-wide consultation.

1.2. External Consultation

- staff representatives through the National Staff Consultative Forum
- Community and Public Sector Union
- the Australian Government Security Vetting Agency.