# Security Clearances

## Instruction and Guideline

<table>
<thead>
<tr>
<th>Published date:</th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Availability:</td>
<td>Internal and external</td>
</tr>
<tr>
<td>Purpose:</td>
<td>To detail the requirement to hold and maintain a security clearance.</td>
</tr>
<tr>
<td>Owner:</td>
<td>First Assistant Secretary Integrity, Security and Assurance Division</td>
</tr>
<tr>
<td>Category:</td>
<td>Executive</td>
</tr>
<tr>
<td>Sub-category:</td>
<td>Leadership and Workforce</td>
</tr>
</tbody>
</table>
| Contact:       | Director, Employment Suitability, Integrity and Professional Standards Branch  
|                | Director, Policy and Reporting, Security Branch |
| File No:       |  |
Table of Contents

Introduction 4

1. Policy statement 4
   Requirement for a Baseline security clearance 4

2. Onboarding 4

3. Applying for a security clearance 5
   Departmental employees 5
   Contractors / consultants 5

4. Security clearance revalidation 5

5. Security clearance waivers 6

6. Security undertakings 6

7. Consequences of a failure to hold/maintain a security clearance 6
   Departmental employees 6
   Contractors and consultants 7

8. Review rights 7
   Failure to maintain an essential qualification 7
   AGSVA decision not to grant a security clearance 7
   APS employees 7
   Non-APS employees and contractors/consultants 7

9. What happens if this Instruction and Guideline is not followed? 7

10. Related policies 8
    Legislation 8
    Other 8

11. Consultation 8
    Internal Consultation 8
    External Consultation 8

12. Endorsement 9

13. Approval 9
Summary of main points

This Instruction and Guideline outlines:

• requirements in relation to security clearances.

This Instruction and Guideline applies to:

• Immigration and Border Protection (IBP) workers¹ who are:
  o ongoing and non-ongoing Australian Public Service (APS) employees in the Department of Home Affairs (the Department)
  o secondees whose services are made available to the Department (including an officer or employee of the APS, a Commonwealth, State or Territory agency or authority, or a foreign government or authority, or a public international organisation)
  o contractors and consultants working ‘in-house’ in the Department (i.e. physically located in premises, or on vessels or aircraft, that are owned, managed, controlled, leased, contracted by or operated by the Department) under a contract for services, other than locally engaged staff at overseas posts (‘Internal contractors/consultants’)
  o all other contractors and consultants working for the Department (‘External contractors / consultants’) who require non-public access² to Departmental Assets³, unless the Assistant Secretary, Integrity and Professional Standards (I&PS) Branch, in consultation with the relevant business area, has determined the individual does not fall within the scope of the Department’s Employment Suitability Screening policy⁴.

• The Secretary of the Department and the Australian Border Force Commissioner.

• Individuals who are not IBP workers but require non-public access to Departmental Assets, unless the Assistant Secretary, I&PS Branch, in consultation with the relevant business area, has determined the individual does not fall within the scope of the Department’s Employment Suitability Screening policy.

¹ Home Affairs workers are referenced as IBP workers under the Australian Border Force Act 2015, which remains consistent post establishment of the Department of Home Affairs. IBP workers are defined in section 4 of the Australian Border Force Act 2015 and the Secretary Determination on IBP workers.

² ‘Non-public access’ means ongoing or unrestricted access to Departmental Assets which are not available to members of the public.

³ Departmental assets includes (but is not limited to) any information and technology systems (ICT systems), information, plant and equipment, vessel, aircraft and / or premises that is owned, operated, managed, controlled, leased or contracted by the Department.

⁴ Business areas must undertake a risk assessment where they believe an individual or group of individuals requires access to Departmental information or resources but should not fall within the scope of the Department’s Employment Suitability Screening policy. Assistant Secretary I&PS Branch will make the final decision in relation to any such assessment.
Introduction

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

Under the Australian Public Service Act 1999 (Cth), agency heads may require a security clearance as a condition of employment. Additionally, under the Protective Security Policy Framework (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.

This Instruction and Guideline sets out the Department’s requirements in relation to security clearances.

This Instruction and Guideline does not affect existing requirements in relation to security undertakings in the Department.

Requirements in relation to employment suitability screening are covered in the Employment Suitability Screening Instruction and Guideline and Associated Documents.

Existing arrangements for locally engaged staff at overseas posts will remain in place for the present.

1. Policy statement

Requirement for a Baseline security clearance

Subject to the timing, conditions and security clearance waivers described below, all individuals who require non-public access to Departmental Assets must obtain and maintain, at a minimum, a 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 (I&PS) Branch, Integrity, Security and Assurance Division.

A Baseline security clearance provides ongoing access to 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 will allow greater efficiency and interoperability. It will also facilitate human resource movement within the Department.

2. Onboarding

From 1 July 2015, subject to security clearance waivers explained below, all new employees and other individuals requiring non-public access to Departmental Assets (other than locally engaged staff at overseas posts) are required to hold a minimum Baseline security clearance before commencement and as a precondition of their engagement.
3. Applying for a security clearance

Departmental employees

Departmental employees who do not currently hold a security clearance must complete and submit a ‘Request to Initiate Security Clearance’ form, which can be accessed on the intranet. If you are unsure as to whether you hold a security clearance, or the level of security clearance required for your position, you can check this using easySAP. If you are not recorded in easySAP as holding a security clearance, you should submit a self-registration form, even if you believe you already hold a security clearance. I&PS Branch will verify with AGSVA whether you hold a security clearance and arrange for easySAP to be corrected where necessary.

Once the self-registration form is received, I&PS Branch will liaise with AGSVA to commence the security clearance process where required.

Once I&PS Branch has notified AGSVA, applicants will be asked by AGSVA to complete a security package comprising:

- security clearance ePack questionnaire—applicants will need to complete and submit this online questionnaire to AGSVA
- 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: http://www.defence.gov.au/agsva/FAQ/clearance-subject.asp

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

It is expected that all Departmental employees will hold at least a Baseline security clearance by 30 October 2015. Compliance with this requirement is being monitored by I&PS Branch.

Contractors/consultants

Contract managers in business or contract management areas must initiate the process for contractors or consultants who require a security clearance. For more information, contact the Employment Suitability team at securityclearances@homeaffairs.gov.au or esc@homeaffairs.gov.au.

4. Security clearance revalidation

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

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

The Secretary of the Department, Deputy Secretary Executive, First Assistant Secretary Integrity, Security and Assurance Division and Assistant Secretary I&PS Branch may, at his or her 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 Branch, 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 Branch (via securityclearances@homeaffairs.gov.au). I&PS Branch will submit the request to the decision maker, as appropriate, for consideration and decision.

6. Security undertakings

It is important to note that a security undertaking is an administrative mechanism only. 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 holds a security undertaking, business areas must comply with relevant policies and legislation regarding access to security classified information.

A security undertaking is separate to and in no way equates to a Commonwealth security clearance. This policy does not affect existing requirements in relation to security undertakings.

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

This Instruction and Guideline does not alter the legal requirements under the relevant legislative framework. Pursuant to the Employment Suitability and Security Screening Secretary Directions of 1 July 2015, made under ss55(1) of the Australian Border Force Act 2015, 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.

Departmental employees

Failure to comply with the Secretary Directions may constitute a failure to adhere to an Australian law and give rise to a breach of the 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 his or her 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).
**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 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 Branch.

**8. Review rights**

**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.

**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.


**9. What happens if this Instruction and Guideline is not followed?**

Departmental employees are reminded that Instructions and Guidelines have the effect of being directions of the Secretary under the *Public Service Act 1999*. Departmental employees must therefore comply with the requirements of this Instruction and Guideline. A failure, neglect or refusal to adhere to the Instruction and
Guideline may give rise to a breach of the Code of Conduct in the Public Service Act 1999, the duties of officials under the Public Governance, Performance and Accountability Act 2013, an offence under the Criminal Code Act 1995, and may result in disciplinary or other appropriate action being taken commensurate with the circumstances and the seriousness of the occurrence.

For contractors and consultants, this Instruction and Guideline must be complied. Failure to comply may constitute a breach of the contract and/or a direction under the Australian Border Force Act 2015.

10. Related policies

- Employment Suitability Screening Instruction and Guideline and Associated Documents
- Declarable Circumstances Instruction and Guideline

Legislation

- Public Service Act 1999
- Australian Border Force Act 2015
- Public Service Regulations 1999

Other

- Australian Government Protective Security Policy Framework
- Australian Government Personnel Security Guidelines

11. Consultation

Internal Consultation

The following internal stakeholders have been consulted in the development of this Instruction and Guideline:

- Integrity, Security and Assurance Division
- Legal Division
- Communication and Media Branch
- Procurement and Contracts Branch
- all staff through Department-wide consultation.

External Consultation

The following external stakeholders have been consulted in the development of this Instruction and Guideline:

- staff representatives through the National Staff Consultative Forum
- Community and Public Sector Union
12. Endorsement

<table>
<thead>
<tr>
<th>Endorsed on</th>
<th>26 June 2015</th>
<th>Signed</th>
</tr>
</thead>
</table>
| By          | Kaylene Zakharoff  
Assistant Secretary  
Integrity and Professional Standards Branch |        |

13. Approval

<table>
<thead>
<tr>
<th>Approved on</th>
<th>26 June 2015</th>
<th>Signed</th>
</tr>
</thead>
</table>
| By          | Jan Dorrington  
First Assistant Secretary  
Integrity Security and Assurance Division |        |
| Period of Effect | 3 years from 1 July 2015 | Review Date | 1 July 2016 |