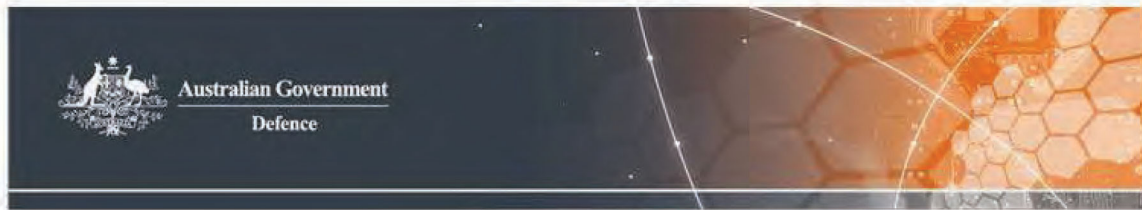


OFFICIAL



Defence Security Principles Framework (DSPF)

Identity Security

General principle

1. Individuals' identities will be verified and, where necessary, protected in relation to association with particular roles and capabilities.

Rationale

2. Proof of identity assists Defence to mitigate risks associated with unauthorised persons accessing Defence establishments or information and reduces the likelihood of fraud.
3. Defence protects the identities of personnel associated with sensitive capabilities to maintain operational security of that capability and the safety of the individual and their family.

Expected outcomes

4. Defence maintains proof of identity processes, requiring individual identities to be verified in accordance with Defence People Group's 'Identity Management Framework';
5. Information relating to Protected Identities is secured appropriately;
6. Defence personnel and persons engaged under a contract are made aware of their roles and responsibilities in relation to Protected Identities;
7. Individuals assigned Protected Identity status conduct themselves in a way that maintains their own personal protection; and
8. Defence personnel and persons engaged under a contract report all such unauthorised disclosures as a security incident.

OFFICIAL

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Assistant Secretary People Policy and Employment Conditions (AS PPEC)
High	Defence Security Committee (DSC) – through AS PPEC
Extreme	Defence Security Committee (DSC) – through AS PPEC

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Document administration

Identification

DSPF Principle	Identity Security
Principle Owner	First Assistant Secretary Defence Security (FAS DS)
DSPF Number	42
Version	2
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 42.1
Control Owner	FASPS&W

Related information

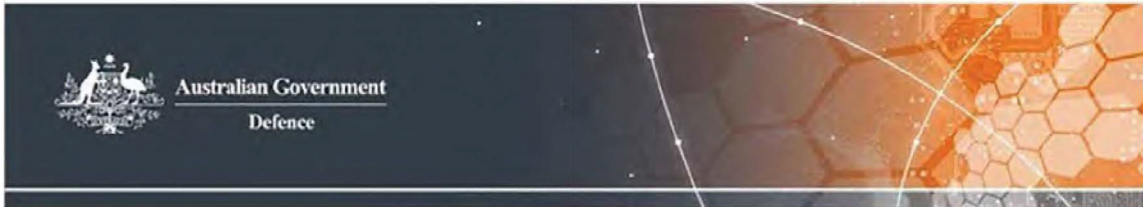
Government Compliance	<p>PSPF Core Requirements: Entity physical resources; and Eligibility and suitability of personnel.</p> <p>Legislation:</p> <p>ASIO Act 1979, Part V section 92</p> <p>Crimes Act 1914, Part IAC Assumed Identities</p> <p>Intelligence Services Act 2001, Part 6, section 41</p> <p>Defence (Inquiry) Regulations 1985</p>
Read in conjunction with	<p>Verification of Identities addressed by Defence People Group's Identity Management Framework.</p> <p>Controls surrounding Protected Identities are addressed in DSPF Control 42.1 – <i>Protected Identities</i></p>
See also DSPF Principle(s)	<p>Classification and Protection of Official Information</p> <p>Information and Technology Security (Personnel)</p> <p>ICT Certification and Accreditation</p> <p>Personnel Security Clearance</p> <p>Overseas Travel</p> <p>Physical Security Certification and Accreditation</p> <p>Security Incidents and Investigations</p>
Implementation Notes, Resources and Tools	<p>Defence People Group's 'Identity Management Framework'</p> <p>Defence Form XP188 – Defence Security Report</p> <p>Annex A to Control 42.1 Protected Identities Defence process for granting honours and awards (including the process for individuals with protected identities).</p> <p>Administrative Inquiries Manual, Chapter 2: Initiating An Inquiry Under The Defence (Inquiry) Regulations 2018.</p> <p>National Identity Security Strategy 2012.</p> <p>National Identity Proofing Guidelines 2014.</p>

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy

~~PROTECTED~~



Defence Security Principles Framework (DSPF)

Protected Identity Information

Control Owner

1. First Assistant Secretary People Services and Wellbeing (FASPS&W) is the Control Owner for this control. The First Assistant Secretary Defence Security (FAS DS) is the Policy Owner for security.

Escalation Thresholds

2. FASPS&W has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	AS People Systems & Payroll Services
High	Defence Security Committee (DSC) – through FASPS&W
Extreme	DSC – through AS FASPS&W

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.

Scope

3. Australian Signals Directorate (ASD) utilises various Defence systems, and this Control also includes ASD's requirements.

4. Protection of identities afforded under the following legislation is outside the scope of this Control:

- a) [Crimes Act 1914](#), Part IAC Assumed Identities;

~~PROTECTED~~

~~PROTECTED~~

- b) past or present employees of the Australian Security Intelligence Organisation (ASIO), see [Australian Security Intelligence Organisation Act 1979](#), Part V, section 92; and
- c) past or present employees of the Australian Secret Intelligence Service (ASIS), see [Intelligence Services Act 2001](#), Part 6, section 41.

Controls

Protected Identity Information

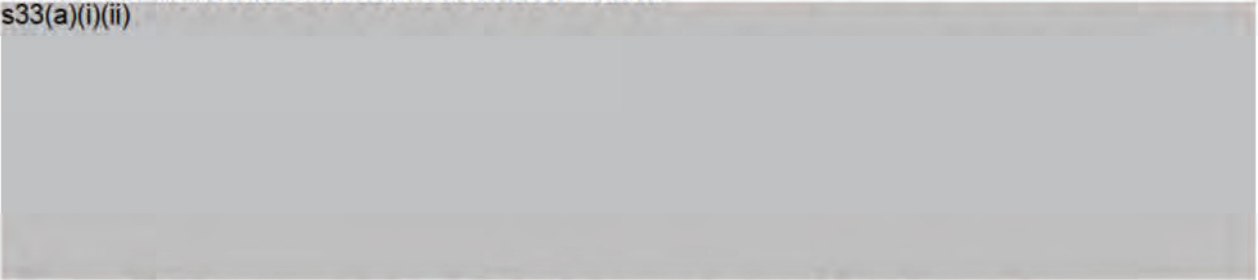
s33(a)(i)(ii)



Purpose of Protected Identity Information Control

7. The purpose of this Control is to safeguard information associated with sensitive capabilities, including both the sensitive capability itself and any details about an individual's direct association with it.

s33(a)(i)(ii)



9. Guidance provided in this Control is not designed for retrospective assignment of protected identity status after an individual's direct connection to a

¹ 'Additional Security Protection' refers to limiting accessibility to the information within Defence IT systems in the Defence Protected Environment. The information remains classified as 'Protected'.

~~PROTECTED~~

~~PROTECTED~~

sensitive capability has ceased. Where Commanders and Managers identify a need to limit exposure of information relating to an individual's previous association with a sensitive capability for privacy, safety, or other lawful reasons, those Commanders and Managers are responsible for applying appropriate Operational Security (OPSEC) and/or privacy measures.

Note: The inclusion of information as Protected Identity Information is distinct from disclosure policy, which is specifically associated with the authority for individuals to make certain protected or sensitive information public either during or upon completion of their Defence employment, and is subject to separate governance.

Unauthorised Disclosure

10. In the course of their employment, Defence and ASD personnel and persons engaged under a contract by Defence or ASD may have contact with individuals who are directly associated with a sensitive capability.

11. Defence personnel, and persons engaged under a contract, must not disclose information related to the role undertaken by an individual directly associated with a sensitive capability granted protected identity status or their family without authorisation from either the DPIIA, FAS Defence Integrity, or the Provost Marshal ADF in the execution of their responsibilities.

Example: When arranging relocation for posting or attachment of a person associated with a sensitive capability, details of that individual's position or role should not be included in the details passed to persons engaged under a contract or other government entities facilitating that relocation. Any personal information provided should be sufficient to ensure efficient service delivery while not enabling the nature of employment to be deduced.

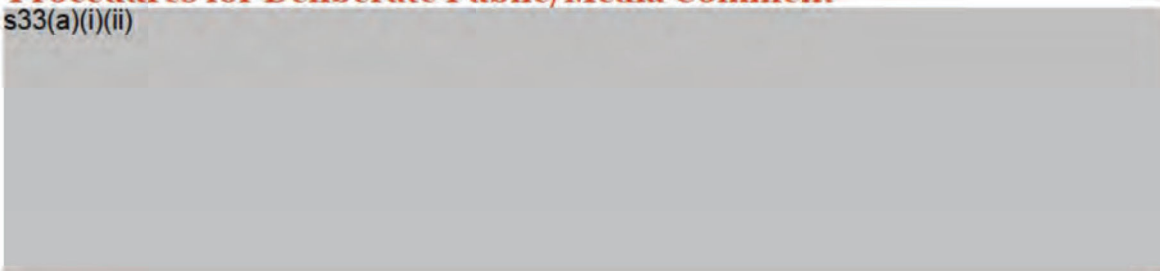
12. Unauthorised disclosures of Protected Identity Information must be reported as follows to:

- a) Defence Security Division as a Security Incident for Defence capabilities, and
- b) ASD Security and Integrity Branch for ASD capabilities.

Note: Disclosure of an identity that is protected by legislation is a criminal matter that will be referred by Defence to the relevant civilian authority for investigation. Where disclosures are not reported and managed, DPIIA are authorised to rescind approvals.

Procedures for Deliberate Public/Media Comment

s33(a)(i)(ii)



~~PROTECTED~~

~~PROTECTED~~

Note: In general, Defence personnel and persons engaged under a contract are not to comment publicly (open forums or discussions) or to the media about Defence or ADF activities and related capabilities without proper authorisation. [Defence Media and Communication Policy – Principle 1 – Releasing official content or making public comment on behalf of Defence must be authorised](#) provides further information.

Information and Communication Technology (ICT) Systems Requirements

s33(a)(i)(ii)

Procedures for Granting Honours and Awards

18. When an individual directly associated with a sensitive capability is to be recognised with an honour or award, OPSEC of the sensitive capability or project, and the protection of Defence personnel and their families is the first priority. This is to always override any desire for public recognition or the gaining of favourable publicity.
19. Information related to an individual directly associated with a sensitive capability; or a sensitive capability must not be released without permission from the relevant DPIIA.
20. Notwithstanding this security consideration, there may be occasions when the release of some information may be appropriate (refer Annex A of this Control - Process for Granting Honours and Awards). In these instances, a public release may be made without disclosing personal information, details of the sensitive capability or work undertaken in consultation with the relevant Group or Service responsible for the capability involved.

~~PROTECTED~~

~~PROTECTED~~

s33(a)(i)(ii)

Involvement in Legal Proceedings

21. Personnel directly associated with a sensitive capability have no additional protection under Australian law for involvement in civil legal proceedings, beyond those protections available to all Australian citizens. Where such an individual is requested to disclose information related to the sensitive role with which they are associated or any other classified information to a Court, the procedures outlined in the DSPF Principle 10 - *Classification and Protection of Official Information* are to be applied.

22. A person with protected identity status is not exempt from requirements of a Court of Inquiry meaning a General Court of Inquiry, a Board of Inquiry (BOI) or a Combined BOI or CDF Commission of Inquiry as set out in the *Defence (Inquiry) Regulations 1985*.

23. If there are issues concerning the potential release, in a Court of Inquiry, of national security classified information, personal information of an individual provided protected identity status, or if such individuals are to be called or involved, they are to be identified in the Scoping Plan. Further information on scoping and planning associated with a Court of Inquiry is included in the [Defence Administrative Inquiries Manual](#).

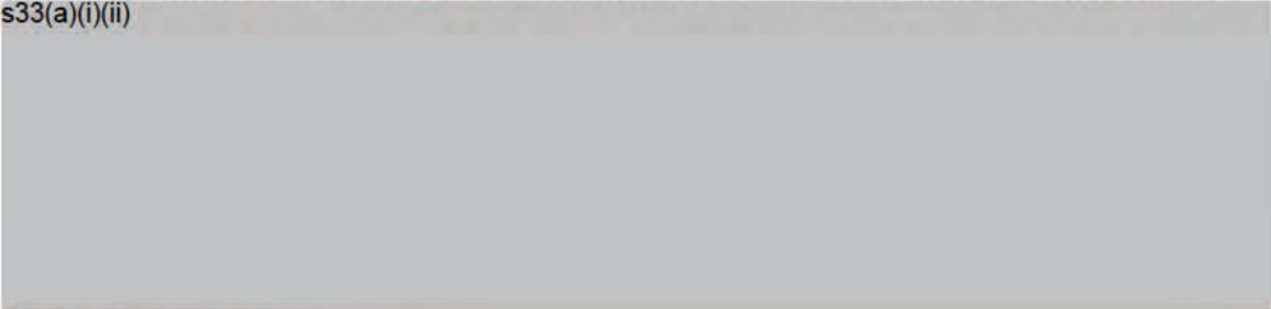
s33(a)(i)(ii)

~~PROTECTED~~

~~PROTECTED~~

Commanders and Managers of Individuals with Protected Identity Status

s33(a)(i)(ii)



Public Affairs Officers

s33(a)(i)(ii)



Key Definitions

35. **Assumed identity.** An identity issued in accordance with the *Crimes Act 1914* Part IAC Assumed Identities. Assumed identities are issued to members of participating agencies in accordance with the provisions of the Act. Defence personnel and persons engaged under a contract may on occasion work with staff from other agencies who are issued with an assumed identity.

~~PROTECTED~~

~~PROTECTED~~

36. **Essential Elements of Friendly Information (EEFI).** Critical exploitable information concerning friendly dispositions, intentions, capabilities, morale, knowledge and potential vulnerabilities that, if compromised, could threaten the success of friendly force.

37. **Protected identity information.** Protected identity information is information deemed by a DPIIA to be:

- a) about a sensitive capability that requires additional security protection through this control, and/ or
- b) about a person's direct association with the sensitive capability.

38. **Sensitive capability.** A capability which, if revealed, could seriously jeopardise operational or reputational effectiveness or place directly associated personnel under unacceptable risk from foreign intelligence services, internal threats, special interest groups or terrorist groups. ^{s33(a)(i)(ii)}

Further Definitions

39. Further definitions for common PSPF terms can be found in the [Glossary](#).

40. Definitions for common Defence administrative terms can be found in the [Defence Instruction – Administrative Policy](#).

Annexes and Attachments

Annex A – Process For Granting Honours and Awards.

~~PROTECTED~~

~~PROTECTED~~

Document administration

Identification

DSPF Control	Protected Identities
Control Owner	FASPS&W
DSPF Number	42.1
Version	3
Publication date	24 October 2024
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Identity Security
Related DSPF Control(s)	Classification and Protection of Official Information Information and Technology Security (Personnel) ICT Certification and Accreditation Personnel Security Clearance Overseas Travel Physical Security Certification and Accreditation Security Incidents and Investigations

Version control

Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS PPEC	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	24 October 2024	AS PS&PS	Redraft commissioned by Defence Security Committee.

~~PROTECTED~~