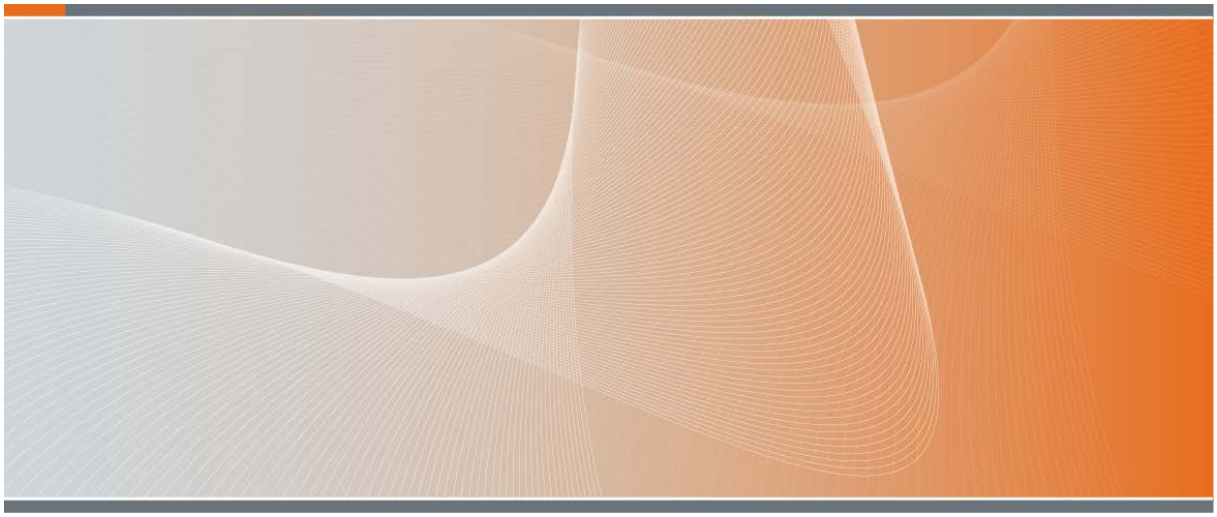
Australian Government
Department of Defence

DEFENCE SECURITY PRINCIPLES FRAMEWORK



Celia Perkins
First Assistant Secretary
Defence Security and Vetting Service
Policy Owner (Security)

Department of Defence
CANBERRA ACT 2600

02 July 2018

Defence Security Principles Framework

Governance and Executive Guidance

Approvals

1. The Defence Security Principles Framework (DSPF) has been endorsed by the Secretary of Defence as the Agency Security Authority for Defence.

2. This document and the related DSPF Principles and Controls have been issued by the First Assistant Secretary Security and Vetting Service (FAS S&VS) with the authority of the Associate Secretary on 2 July 2018.

Purpose

3. The DSPF aligns Defence with the Commonwealth's Protective Security Policy Framework (PSPF). Under the PSPF all agencies must develop their own protective security policies and procedures.

Objective

4. The DSPF is a principles-based framework intended to support a progressive protective security culture that understands and manages risk, leading to robust security outcomes. This approach:

- Allows all parts of Defence to manage security within their operational context and constraints. This recognises the best security decisions are made in accordance with agreed principles, with a desired outcome in mind.
- Ensures the most appropriate people are setting security requirements. Those who know their business are best placed to set security standards and requirements for that aspect of Defence business.
- Sets clear processes and accountabilities, which underpin assurance of Defence protective security arrangements.

Scope and applicability

5. This document, and all documents that belong to the DSPF (DSPF documents), are administrative policy framework documents. They apply to all Defence personnel.

6. The terms of a relevant contract may extend the application of DSPF documents to a contractor, consultant or outsourced service provider.

7. The Secretary and the CDF require Defence personnel to comply with provisions in DSPF documents unless the particular circumstances warrant departure from the provisions.

8. Some provisions in framework documents may support Defence personnel to comply with obligations that exist in:

- Applicable laws
- The *Defence Enterprise Agreement*
- Directives and determinations issued under the *Public Service Act 1999* or the *Defence Act 1903* or the *Defence Enterprise Agreement*

  or

- Defence Instructions.

9. Defence personnel must not depart from the provisions in framework documents in a way that would result in any breach of those obligations.

10. When considering a possible departure from DSPF documents the Secretary and the CDF require Defence personnel to:

- Consider whether the proposed departure would be inconsistent with:
  - Applicable laws
  - The *Defence Enterprise Agreement*
  - Directives and determinations issued under the *Public Service Act 1999* or the *Defence Act 1903* or the *Defence Enterprise Agreement*

    or

  - *Defence Instruction – Administrative policy* and other extant Defence Instructions.

  If yes, the departure is not permitted;
- Consider whether a proposed departure is reasonable and justified in the circumstances and will produce a better outcome for Defence.
- Consult their supervisor, wherever practicable, about a proposed departure – a properly informed decision also involves consulting the policy owner.

- Be responsible and accountable for the consequences of departing from, or not adhering to, the content of DSPF documents including where such departure or non-adherence results in a breach of applicable laws or leads to adverse outcomes for Defence.

11. Defence personnel may be subject to performance management, administrative action or, in some circumstances, disciplinary action where their decision to depart from provisions in DSPF documents involves serious errors of judgement.

12. Failure to adhere to administrative policy may result in a breach of legislation or other legal requirement and sanctions under that legislation may apply.

13. Defence personnel who award or manage contracts should consider whether there is a specific and documented reason to include in the terms of a contract the requirement to comply with the provisions of DSPF documents and, if so, include such terms.

14. Failure by a contractor, consultant or outsourced service provider to comply with the requirements of this policy – where compliance is a term of the contract – may result in a breach of contract.

DSPF Document management and availability

15. DSPF documents belong to the administration and governance policy domain in the administrative policy framework. The Associate Secretary is the accountable officer and the FAS S&VS is the policy owner for security. The policy contact is the Enterprise Security Policy and Advice section within the Defence Security and Vetting Service: dspf.development@defence.gov.au

16. The DSPF is a flexible policy framework. DSPF documents will be reviewed and updated as necessary from 02 July 2018.

17. Authoritative DSPF documents are only available from the interactive DSPF site on the Defence Restricted Network. A non-interactive version is also available from the DRN Defence manuals site and the Defence Online Services Domain. The currency of DSPF documents cannot be guaranteed if sourced from other locations.

The structure of the DSPF

18. Building on the PSPF and Information Security Manual (ISM), the DSPF provides governance, principles, policy, process and guidance to enable and empower Defence personnel to make security decisions in accordance with risk.

19. The DSPF has three Defence-specific levels of protective security management:

PSPF Whole of Government	Directive on Security of Government Business
	Protective Security Core Requirements and Policies
	Protective Security Protocols
Defence	DSPF Governance and Executive Guidance
	DSPF Principles and Expected Outcomes
	DSPF Controls, Processes and Instructions – including Enterprise-wide Controls

See PSPF and DSPF structure chart

20. The Defence specific guidance will be provided through a suite of documents that will reference, and be subordinate to, the PSPF. The three tiers of Defence Guidance are:

- 4a *DSPF Governance and Executive Guidance*: This document establishes and explains the DSPF framework.
- 4b *DSPF Principles and Expected Outcomes*: These documents provide security principles and expected outcomes across the Defence Enterprise (including references to any guidance, policies, or laws relevant to understanding/applying the principle or achievement of the expected outcome).
- 4c *DSPF Controls, Processes and Instructions*: Where necessary, these documents provide additional controls, processes and instructions relating to the interpretation and the application of DSPF Principles and Expected Outcomes (4b documents) relating to specific, complex or unconventional circumstances. They may also be used to manage circumstances where a degree of commonality across security management would be preferable and beneficial. It is neither expected, nor desirable, that all *DSPF Principles and Expected Outcomes* (4b) have accompanying *DSPF Controls*, *Processes and Instructions* (4c documents).

Understanding Principles and Expected Outcomes

21. *DSPF Principles and Expected Outcomes* (4b) follow a standard format. Each includes:

- The Principle: the high-level statement of intent (this is *what* we need to do);
- The Rationale: a statement explaining the importance of the principle (this is *why* we do it); and

- The Expected Outcomes: a statement of what needs to be achieved in order to meet the intent of the principle (this is Defence's desired *end* state).

22. *DSPF Principles and Expected Outcomes* documents do not include specific steps on how security outcomes should be achieved. Rather, they outline basic principles and desired outcomes that should guide our design and implementation of policy and controls to effectively manage security risks.

Constraints, Obligations and External Requirements

23. The DSPF has been designed around the concept of managed flexibility. This means that decision makers will have flexibility to adapt security solutions to their context. However, risk management decisions must also be shaped/influenced by relevant guidance, policies, or laws, such as:

- Legislation and regulation;
- Whole of government policy and expected outcomes;
- Decisions of relevant senior leadership, committees and boards;
- Australian and International standards; and
- International obligations and agreements.

24. Each DSPF principle document contains a "See also" section and an "Implementation Notes, Resources and Tools" section to provide applicable external implementation guidance.

Understanding controls, processes and instructions (4c)

25. Where additional guidance is needed to manage or mitigate a security risk beyond the general principle provided in the 4b documents, it may be appropriate to develop a 4c document which provides controls, processes and instructions.

26. Controls, processes and instructions are developed by **Control Owners**, an SES or ADF Star Rank Officer assigned accountability and authority to manage a specific defence security risk (refer paragraph 56).

27. Controls, processes and instructions, need to be sufficiently detailed to meet the security objective, but should not be so prescriptive as to produce a compliance based approach to security – except where there is a basis for a mandatory direction (refer paragraph 33).

28. **Control Owners** may set *DSPF Enterprise-wide Controls* (4c). Other types of 4c control processes and instructions may be Group or Service specific, collaborative or locational. These should be approved by the relevant **Control Owner**.

Security Controls Guidance

29. Security controls, processes and instructions need to be formally documented as they may be subject to review or audit. Security related decisions should be recorded in approved Defence records management systems accordance with Records Management Policy Manual and guided by Good Decision-Making in Defence.

Reviewing Controls, Processes and Instructions

30. Controls, processes and instructions, and security decisions more broadly, may need to be reviewed; in line with continuous improvement and best practice. The requirement exists to review *DSPF Controls, Processes and Instructions*, and consult stakeholders, to support and ensure effective security risk management practices:

- following a significant incident;
- following a change in environment or risk context; or
- as part of a scheduled program of review or audit.

Risk Management

31. Security risks should be resolved at the lowest possible level. All Defence personnel have an obligation to evaluate and treat risks. Serious residual risks, informed by a Security Risk Assessment, need to be escalated to the appropriate decision-maker for management. Business Impact Levels (BILs) should be used to assess the impact of the loss of information or assets.

32. Security risks are managed under the DSPF through:

- escalation of serious residual risks; and
- regular reporting.

Mandatory Provisions

33. Some provisions in the DSPF are mandatory. These are identified through the use of the word **must** and **must not** (bold type).

34. Any mandatory provision under the DSPF is to be approved by the Agency Security Adviser (ASA). They are authorised under the Defence Instruction Administrative Policy and non-compliance is a reportable security incident. Dispensations should only be sought in exceptional circumstances. They will be approved by the relevant Control Owner.

Escalating and Accepting Risks

35. Where there is a risk to achieving the Expected Outcomes of a *DSPF Principles and Expected Outcomes* document, Defence personnel should manage or escalate this risk in accordance with sound risk management practices and the Defence Instruction Administrative Policy. Contractors, Consultants and Outsourced Service Providers cannot manage or escalate risks except through Defence personnel.

36. To enable sound risk management, **Control Owners** should set and make available general thresholds for escalation of serious risks, and specific thresholds on matters of special concern. These thresholds should help Defence personnel to decide which risks to escalate within their Group or Service and which need to be escalated to the Control Owner. The Control Owner also determines which risks need to be taken to the **Defence Security Committee** (**DSC**, refer paragraph 54).

37. Escalation thresholds should determine the level (i.e. rank or position title) at which Defence personnel can manage risks at varying risk ratings (i.e. low to extreme risks).

38. With the exception of mandatory provisions, Defence personnel, Contractors, Consultants and Outsourced Service Providers should regard *DSPF Controls, Processes and Instructions* (4c) policy as guidance. Accepting the risk of departing from policy is to be guided by the escalation thresholds.

39. Where risk management results in a significant departure from Commonwealth policy (the PSPF or the ISM) this is to be reported via Control Owners to FAS S&VS or the CISO for review of impact on obligations to the Commonwealth.

40. The preferred method for assessing risk is the Security Risk Assessment Guide (the SRA Guide). The preferred method of expressing risks and setting a threshold for escalation are the Guide's Risk Rating table and Consequence Descriptors.

41. Where a **Control Owner** already has a mature risk methodology in place they should utilise this, however they should ensure that relevant **Control Implementers** (refer paragraph 60) and **Control Officers** (refer paragraph 63) are aware of the requirement to use this methodology. The **Control Owner** should also map their methodology to the Guide's Risk Rating table.

Regular Reporting

42. The Secretary has an obligation to report annually to Government on Defence compliance with the PSPF. The **Defence Security Risk Steward** must provide an enterprise-wide view of Defence's security risk to the EBC and is the Accountable Officer for security under the Defence Administrative Policy framework.

43. The enterprise-wide security risk view is underpinned by assurance reporting from **Control Owners** (refer paragraph 56). Control Owners are required to provide an annual report to the DSC on each *DSPF Principle and Expected Outcome* (4b) they have responsibility for by completing the DSPF Reporting template. The purpose of this report is to:

- Provide general assurance to the DSC that a specific principle and expected outcome (4b) is being implemented across Defence in a manner that manages the relevant security risks;
- Highlight any serious security incident or events; and
- Raise matters or serious risks of concern for DSC consideration.

44. In addition to an annual report, **Control Owners** should elevate serious residual security risks for action or acceptance by the DSC as they arise. Regular reports can then be used to review the management of serious residual risks.

45. DSPF reporting should be supported by an assurance framework established by each **Control Owner** with relevant **Control Implementers**. This exact nature of this framework will vary from one Control to another. **Control Implementers** will provide appropriate assurance to owners and escalate risks in accordance with defined thresholds.

Training and Awareness

46. Security awareness training is an important element of any protective security regime. It supports the implementation of good policies, practices and procedures and helps to foster positive security attitudes.

47. To support a robust and positive security culture, Defence personnel, Contractors, Consultants and Outsourced Service Providers are to undertake suitable security training for:

- Annual Security Awareness; and
- The appropriate document handling course.

48. Further guidance regarding suitable security training can be obtained from the DS&VS Security Education intranet site.

Roles and Responsibilities

49. The Secretary is responsible for Defence's protective security. This role is assigned through the Attorney-General's Directive on the Security of Government Business. To achieve this, the Secretary is to apply the PSPF, putting effective protective security programs into place that ensure:

- Defence's capacity to function;
- confidence in the department and the Australian Defence Force (ADF) by the public;
- the safeguarding of official information and security-protected assets; and
- the safety of Defence's personnel, contractors, consultants, outsourced service providers and clients.

See DSPF Accountability Diagram

50. The Secretary is the **Risk Owner** of Defence security and, in accordance with the PSPF, has designated:

- The Associate Secretary as the **Defence Security Risk Steward** and the **Agency Security Executive** (**ASE**).
- The FAS S&VS as the appointed **Defence Security Risk Adviser** and the **Agency Security Adviser** (**ASA**).
- The Chief Technology Officer, Chief Information Officer Group, (CIOG) as the **Chief Information Security Officer** (**CISO**) for Defence responsible for providing ICT security.
- The Director-General of the **Australian Signals Directorate** (**ASD**) is the accreditation authority for TOP SECRET Special Compartment Information Facilities (SCIFs) and is the Communications Intelligence Security Authority for Defence.

Defence Security Risk Steward

51. The Associate Secretary is delegated responsibility by the Secretary for Defence security risk management. This includes:

- Implementation of a Defence Security Principles Framework for the management and reporting of security risks in Defence;
- Chairing the **Defence Security Committee** (**DSC**), refer paragraphs 54 and 55; and

- Reporting on the risk and effectiveness of controls, through the DSC, to the **Enterprise Business Committee** (**EBC**).

Defence Security Risk Adviser

52. The FAS S&VS is the **Security Risk Adviser** and provides enabling services in support of enterprise level controls. This includes:

- Maintaining the *DSPF Governance and Executive Guidance* (4a);
- Maintaining *DSPF Principles and Expected Outcomes* (4b) not related to ICT security;
- Appointment of Control Owners
- Providing reporting on enterprise security risk management to the **Defence Security Risk Steward**, for **DSC** and to the **EBC**; and
- Providing Agency input to PSPF and other whole-of-government security compliance reporting.

Chief Information Security Officer

53. The Chief Technology Officer (within CIOG) is the **CISO** responsible for providing ICT security related whole of Defence strategic direction, reporting and advice to the Associate Secretary. This includes:

- Maintaining *DSPF Principles and Expected Outcomes* (4b) related to ICT security.

Defence Security Committee

54. The DSC is chaired by the **Defence Security Risk Steward** and reports to the **Risk Owner** via the EBC.

55. DSC provides the primary oversight of the DSPF. **DSC** members:

- Provide security risk management strategic direction;
- Address escalated residual security risks;
- Consider **Control Owner** (refer paragraph 56) and enterprise-wide security risk reports; and
- Seek to resolve any security related risks, problems or disagreements.

Control Owner

56. An SES or ADF Star Rank Officer assigned accountability and authority to manage a specific defence security risk. These will be derived from the *DSPF Principles and Expected Outcomes* (4b). The relevant **Control Owner** in each instance may be a Group Head or Service Chief, or a more appropriate subordinate.

57. **Control Owners** will:

- Manage, monitor and report on the implementation across the Defence enterprise of any *DSPF Principles and Expected Outcomes* (4b);
- Set relevant *DSPF Enterprise-wide Controls* (4c);
- Approve other categories of *DSPF Controls, Processes or Instructions* (4c) for Group or Service specific, collaborative or locational purposes;
- Define **Control Implementers** (refer paragraph 60) and establish any necessary horizontal accountability arrangements, including oversight of subordinate 4c documents;
- Build a framework and culture for the resolution of risks at the lowest possible level;
- Act as Enterprise Subject-Matter Expert for relevant *DSPF Principles and Expected Outcomes* (4b);
- Provide appropriate assurance and reporting to the **DSC** and the **Security Risk Steward**;
- Set and make available general thresholds for escalation of serious risks, and specific thresholds on matters of special concern; and
- Escalate risks that have a significant impact on the residual security risk to the **DSC** (in this sense a **Control Owner** is also a manager of residual risk).

58. **Control Owners** will be proposed to implement *DSPF Principles and Expected Outcomes* (4b) as required by FAS S&VS on the basis of:

- Formal organisational responsibility/accountability;
- Expertise; and
- Control of resources.

59. Where a **Control Owner** cannot be agreed the ownership will be referred to the **DSC** (refer paragraph 54).

Policy Owner and Publishing Authority

While **Control Owners** are responsible for the setting of any *DSPF Enterprise-wide Controls* (4c), FAS S&VS is the Policy Owner and the DSPF publishing authority. When developing individual 4c guidance the **Control Owner** must meet *DSPF Principles and Expected Outcomes* (4b). Relevant 4c **Control Owners** can approve variations to a 4c Control in accordance with good policy practices such as appropriate consultation. Further guidance can be obtained from the Directorate of Administrative Policy and the Better Policy Handbook.

Control Implementer

60. Group Heads and Service Chiefs, or Commanders and Managers of specific business units, may be specifically delegated responsibility by the **Control Owners** to ensure the implementation and/or reporting against specific controls to mitigate or manage security risks. They will generally be the managers or commanders with some specific responsibility for the implementation of the 4c Control.

61. **Control Implementers** will:

- Implement *DSPF Enterprise-wide Controls* (4c) within their business unit;
- If required, develop subordinate DSPF controls, processes or instructions (4c) that are Group/Service specific, Collaborative or Locational (such as Standard Operating Procedures);
- Provide reasonable assurance and reporting to **Control Owners**;
- Promote the resolution of risks at the lowest possible level; and
- Elevate significant security risk concerns with relevant **Control Owners**.

62. **Control Implementers** will be formally designated by **Control Owners**.

Control Officers

63. **Control Officers** encompass all staff and stakeholders in the Defence Enterprise. Defence personnel, contractors, consultants and outsourced service providers all have a duty to manage security risk in accordance with the DSPF.

64. Supervisors and custodians of information and assets are accountable for the appropriate implementation of DSPF principles, policies, processes and controls within their work places.

65. Where Defence personnel outsource a function, they cannot outsource the risk. Commanders and managers remain accountable (via the contract manager) for

the protective security of their function and any official information and sensitive equipment made available to Contractors, Consultants and Outsourced Service Providers.

Accountability and Relationships between Roles

Control Officers and **Control Implementers** can be accountable to **Control Owners** outside of their Group/Service (horizontal accountability). **Control Owners** can designate **Control Implementers** regardless of their Group or Service, and will set clear expected outcomes for **Control Implementers** to manage and improve security controls in accordance with security risk assessments.

Effective communication will be vital, as horizontal accountability is critical to effective enterprise security management. Where horizontal accountability raises risks or concerns, **Control Owners** should seek a mutually agreed outcome about the **Control Implementers** role. If an agreement cannot be reached the matter should be escalated to the **DSC**.

Executive Security Advisers

66. Each Group or Service is to appoint an **Executive Security Adviser** (**ESA**). The **ESA** will:

- Support their senior management, **Control Owners** and **DSC** representatives to analyse their security environment and counter unacceptable risks;
- Act as their Group or Service point of contact for security matters;
- Support their Group or Service in maintaining an effective **Security Officer** structure; and
- Provide advice to their Group and Service **Security Officers**, **Control Implementers**, and **Control Officers**.

Security Officers

67. **Security Officers** are an important part of the Defence Security Community and contribute to the protection of Defence's people, information, assets in support of its capabilities and mission. The role of the **Security Officers** is critical to ensure the desired protective security culture is promoted and maintained across Defence.

68. Security Officers are required to provide DSPF advice and support to **Control Implementers**, **Control Officers**, and their Commanders and Managers on security matters, particularly on the implementation of DSPF principles, policies, processes and controls.

69. Commanders and Managers are to appoint **Security Officers** wherever classified information or security protected assets are stored or handled. They should be appropriately trained (see the DS&VS Security Education intranet site for current Security Officer training requirements) and hold an appropriate security clearance.

70. Defence Industry Security Program (DISP) member executives are to appoint **Security Officers** to support contractual DISP member security obligations. Commanders and managers are not to appoint an external service provider as a security officer and DISP member executives are not to appoint a sub-contractor as a **Security Officer**.

Contents

Defence Security Principles Framework (DSPF)

Classification and Protection of Official Information

General Principle

1. Defence will protect Official Information in accordance with the expectations of the originator of the information. Where Defence is the originator of information, it will classify that information, according to the impact of access by, or disclosure to, unauthorised individuals, groups or organisations.

Rationale

2. The security of information is critical to the integrity of Defence's mission. If Defence does not protect its own information and information received from external parties from unauthorised access, its ability to function in support of the Government will be undermined. The security classification system allows Defence to share and exchange information with confidence by ensuring a common recognition of confidentiality requirements and the consistent application of protective security measures.

Expected Outcomes

3. The criteria and processes that Defence uses to assess and classify information are consistent with the requirements set out in the Protective Security Policy Framework. This security classification assessment will be informed by a broader assessment of Business Impact Levels (BILs) on each occasion.

4. Suitable controls are applied to Official Information to ensure that it is protected from unauthorised access or disclosure.

5. Defence protects foreign government information received under a General Security Agreement (GSA) or Defence-specific Security of Information Agreement or Arrangement (SIA) in accordance with the relevant terms.

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	AS SPS
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Classification and Protection of Official Information
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 10
Version	2
Publication date	31 May 2019
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 10.1
Control Owner	Assistant Secretary Security Policy and Services

Related information

Government Compliance	**PSPF Core Requirements:** Sensitive and classified information; and Access to information. **Legislation:** *Freedom of Information Act 1982* (Cth) *Privacy Act 1988* (Cth)
See also DSPF Principle(s)	Information Systems (Physical) Security Information Systems (Personnel) Security Personnel Security Clearance Overseas Travel Working Offsite Physical Transfer of Information and Assets
Implementation Notes, Resources and Tools	Business Impact Levels FAQ, tools and guide

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 May 2019	FAS S&VS	Foundational review; PSPF update; and security classification alignment.

Defence Security Principles Framework (DSPF)

Classification and Protection of Official Information

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this Enterprise-wide Control.

Control

2. This section of this DSPF Enterprise-wide Control is For Official Use Only and has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – *Selecting an Appropriate Protective Marking*

Annex B – *Applying Protective Marking to Official Information*

Annex C – *Reviewing and Altering Protective Markings*

Annex D – *Release of Official Information*

Annex E – *Registration of Protectively Marked Information*

Annex F – *Official Information Filing and File Census*

Annex G – *Copying and Reproduction of Protectively Marked Information*

Annex H – *Disposal and Destruction of Protectively Marked Information and Assets*

Annex I – *Remarking Information Bearing Former Security Classifications*

Annex J – *Certification and Accreditation Appointments*

Document administration

Identification

DSPF Control	Classification and Protection of Official Information
Control Owner	AS SPS
DSPF Number	Control 10.1
Version	2
Publication date	31 May 2019
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Classification and Protection of Official Information
Related DSPF Control(s)	Information Systems (Physical) Security Information Systems (Personnel) Security Personnel Security Clearance Overseas Travel Working Offsite Physical Transfer of Information and Assets

Version control

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

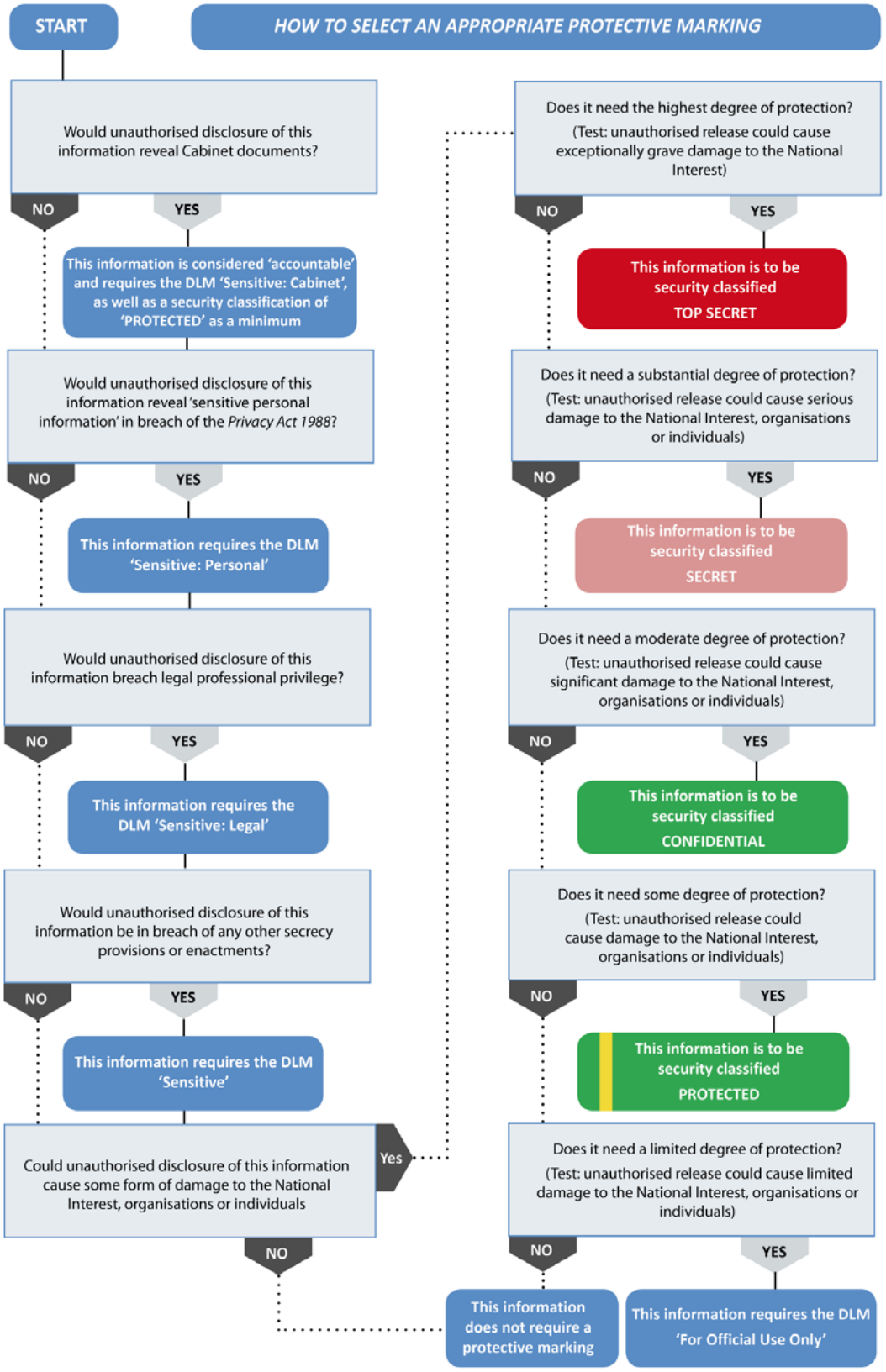
Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.

Defence Security Principles Framework (DSPF)

Annex A to Classification and Protection of Official Information – Selecting an Appropriate Protective Marking

1. The flow chart on the following page outlines the steps involved in selecting the most appropriate protective marking for a document. It remains extant for Defence use, and will be reissued by no later than 1 October 2020 once Defence has transitioned to the revised security classification system.

Figure 1 – Protective marking selection



Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Selecting an Appropriate Protective Marking
Annex Version	2
Annex Publication date	31 May 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Classification and Protection of Official Information
DSPF Number	Control 10.1

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 SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.

Annex B to Classification and Protection of Official Information – Applying Protective Marking to Official Information

1. Where a Protective Marking is required it **must** be clearly marked. In the context of verbal briefings or discussions, it is recommended that the level of the brief or discussion be clearly stated.

Applying Protective Markings to Documents

2. Protective Markings are required to be in capitals, in bold text and of a minimum height of 5mm at the top and bottom of each page. It is recommended that the protective markings are in red.

3. If an existing document requires its Protective Marking to be over stamped, it is recommended that the overstamping be in red.

Applying Paragraph Markings

4. It is recommended that individual paragraphs of a document be protectively marked. Where paragraph markings are used, all paragraphs in the document are required to be marked, so as to avoid a situation where it cannot be determined if a paragraph was intentionally left unmarked in the classification process.

5. The paragraph marking is to appear in a consistent position on each paragraph throughout the document. It is recommended that it is placed in brackets at the beginning of each paragraph. The protective marking can be written in full or abbreviated. Classifications and Dissemination Limiting Markers (DLM) are abbreviated as follows:

a. TOP SECRET (TS)

b. SECRET (S)

c. CONFIDENTIAL (C)

d. PROTECTED (P)

e. Sensitive:Cabinet (Cab)

f. Sensitive:Personal (Pers)

g. Sensitive:Legal (Legal)

h. Sensitive (Sens)

i. For Official Use Only (FOUO)

j. UNCLASSIFIED (U)

6. It is recommended that a paragraph marking key be used in all paragraph marked documents.

Translating New Security Classification Protective Markings

7. During the transition period to the new security classification system, Defence will be able to receive classified information from other federal government departments and agencies that are already using the new security classification system. While the appropriate selective marking for this information will already have been identified by the originator, there will be circumstances in which Defence will be required to identify a Protective Marking different to that selected by the originator.

8. In this case, the equivalencies identified in Table 2 of Control 10.1 - *Classification and Protection of Official Information* **must** be used to determine what Protective Marking is appropriate.

Example: *Emails received with the Protective Marking of OFFICIAL will need to be handled by Defence as UNCLASSIFIED.*

Protectively Marking Titles

9. It is recommended that the title of protectively marked information be UNCLASSIFIED, where possible. If the title needs to be classified, the relevant Protective Marking is to appear abbreviated in brackets after the last word of the title. To enable unclassified reference to such a document, it is recommended the originator apply either an unclassified abbreviated title or reference number and date.

Printed Graphic Material

10. For maps, drawings and other printed graphic material the Protective Marking is to be printed or stamped near the map scale or drawing numbers as well as printed at the top and bottom centre of the document. If the material is to be folded, the marking is to remain visible after folding.

Security Classifying Annexes, Appendices and Covering Documents

11. Sometimes the annex or appendix to a document requires a different security classification from the document itself. If the annex or appendix has a higher

classification than the principal document, the document's front cover is to indicate that the document and the annex or appendix as a whole cover a higher classification.

Example: *CONFIDENTIAL-covering-TOP SECRET*

Example: *UNCLASSIFIED-covering-PROTECTED*

12. If a summary or covering letter to a document does not require any security classification, or has a lower Protective Marking than the document to which it is attached, the summary may remain unclassified or carry a lower Protective Marking. However, it is to indicate that it covers a document of a higher classification.

Example: *UNCLASSIFIED-covering-CONFIDENTIAL*

13. Documents with covers, such as books, pamphlets and reports, are to show the Protective Marking on the front cover, title page and rear cover. Any binding or fastening of pages cannot obscure the Protective Marking.

Aggregation

14. Large compilations of classified information, for example a collection of electronic records, may require the application of higher or additional security controls than individual documents or pieces of information within the compilation. This is because the business impact from the compromise of confidentiality, loss of integrity or unavailability of the aggregated information would cause greater damage than that of individual documents, refer Table 1 of Control 10.1 - Classification and Protection of Official Information for further information on Business Impact Levels.

Imagery

15. Photographs and film requiring security classification and their storage envelopes or containers are to carry a conspicuous Protective Marking. In addition to having Protective Marking on both sides of containers and spools, security classified imagery (including roll imagery, cine-film, video tape) requires a Protective Marking in the title and end sequences to ensure projection of the marking for at least five seconds for each. Photographic negatives are required to be marked to ensure the Protective Marking will be reproduced on all copies made from that negative. The copies are to be marked.

Presentations

16. Security classified presentations are to be protectively marked. Each slide or screen is to be treated as an individual page, as with a paper based document, and marked accordingly. Dot points may be protectively marked in line with paragraph markings. It should also be noted that the speaker's notes in the slides may also contain classified information and these are to be marked accordingly.

Audio

17. For audio presentations and recordings, the level of Protective Marking is to be clearly stated at the beginning and end. The tape or other media and its container is to be conspicuously labelled with the appropriate Protective Marking.

Microforms

18. All microforms such as aperture cards, microfiche and microfilm containing security classified matter are to show the appropriate Protective Marking at the top and bottom centre of each frame. Containers and envelopes are to bear the appropriate Protective Marking. The Protective Marking is to be visible without projection on both aperture cards and microfiche, and microfilm is to be prominently marked at the beginning and end of each roll.

Electronic Storage Media and ICT Equipment

19. Policy for the marking of electronic storage media and devices is contained in:

a. DSPF Principle 22 - *Mobility Device Security*; and

b. the Information Security Manual (ISM).

20. Cryptographic Controlled Items and some other High Assurance products have special labelling requirements in order to maintain tamper evidence. These are detailed in DSPF Principle 13 - *Communications Security (COMSEC)* and its references.

Document administration

Identification

DSPF Annex	Applying Protective Markings to Official Information
Annex Version	2
Annex Publication date	31 May 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Classification and Protection of Official Information
DSPF Number	Control 10.1

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 SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.

Defence Security Principles Framework (DSPF)

Annex C to Classification and Protection of Official Information – Reviewing and Altering Protective Markings

Reviewing a Protective Marking

1. It is recommended that protectively marked information be reviewed after an event such as:

a. the completion of an operation, program or project;

b. a security incident related to the information;

c. a file is withdrawn from use or returned to use; or

d. a muster is conducted.

2. All Defence personnel, Contractors, Consultants and Outsourced Service Providers are encouraged to challenge any security classification they believe is insufficient, excessive or inaccurate by contacting the originator or the business unit responsible for the document or item carrying the classification. A reason for a challenge is to be provided along with a request for declassification or reclassification.

Altering a Protective Marking

3. Only the originator can authorise the alteration of the Protective Markings. Where the originating military or business unit within Defence no longer exists, or if it no longer has the subject matter expertise to make such decisions, the responsibility for reviewing and, if required, altering a Protective Marking rests with the:

a. military or business unit that has assumed the functions and responsibilities of the original unit;

b. Executive Security Adviser (ESA) if it is unclear who has assumed the responsibilities within a Group or Service; or

c. First Assistant Secretary Security and Vetting Service (FAS S&VS) if an appropriate Group or Service cannot be identified as holding the functions

and responsibilities of the original unit. The FAS S&VS may delegate this authority if required.

***Note**: The responsibility as the originator belongs to the functional position from which the information was originally prepared, not necessarily the individual who prepared the document.*

4. For printed material, the Protective Marking is to be changed by crossing out the previous marking and clearly labelling or stamping the new marking. The originator is to then sign and date the front page and note the authority for the change. All copies of the reclassified information are to be amended in the same way. The alteration can be performed by the holders of the information after having received written authorisation from the originator. Form XC040 (Classified Document Register) is to also be amended when the Protective Marking is altered.

5. **Downgrading or Declassification of a document**. Form XC021 - *Downgrading or Declassification of Classified Documents* is to be used when downgrading or declassifying a document that is classified PROTECTED or higher. Users are to follow the instructions contained within Form XC021.

6. **Electronic Records**. The same principles apply when altering the Protective Markings of an electronic record. In this instance, the metadata is amended to reflect the new Protective Marking.

7. **Files**. The registry **must** be informed when a file needs reclassification due to the removal or addition of classified information. If classified information added is of a higher nature than the file, the file classification **must** be upgraded. The file cover is to be temporarily amended until such time the file is returned to the registry, where a change will be made to its Protective Markings.

8. Removal of any information from a file is to be completed in accordance with Defence Records Management Policy. For further information, refer to the Records Management Policy Manual (RECMAN).

9. **Archives**. The NAA or the Australian War Memorial in consultation with the Director of Classified Archival Records Review (DCARR) will review information in the open period that is the subject of a public access request under the *Archives Act 1983*. The DCARR may also review protectively marked archival material as part of a proactive program in anticipation of public access requests under the *Archives Act 1983*. Refer to RECMAN for further information.

***Note**: The DCARR does not provide a general declassification service for Defence. Where a work group requires advice on the continuing sensitivity of a particular topic for a record that is more than 15 years old, DCARR may be able to assist.*

***Note**: If the record is more than 15 years old, a person may be guilty of an offence under the Archives Act 1983, s26(1)(c) if the classification is altered without the permission of the NAA.*

10. If the archival records are held by a service history unit, then that unit will be responsible for reviewing the information of their service only. Joint service records are to be reviewed in liaison with the relevant Service work groups.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Reviewing and Altering Protective Markings
Annex Version	2
Annex Publication date	31 May 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Classification and Protection of Official Information
DSPF Number	Control 10.1

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 SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.

Defence Security Principles Framework (DSPF)

Annex D Classification and Protection of Official Information – Release of Official Information

1. Official Information can include public sector information sanctioned for public access or circulation, such as websites.

2. The authorisation for the release of Official Information is to be managed in accordance with:

a. the Defence Web Estate Manual (WEBMAN) where information is being released on the internet; and

b. in compliance with the *Privacy Act 1988 (Cth)* when personal information is involved.

Other Australian Government Agencies

3. Official Information owned or originated by Defence can be released to other Australian Government agencies that are subject to the Australian Government Protective Security Policy Framework (PSPF), unless the originator has placed any limitations on its release to the contrary. If there is any doubt, the originator's approval is to be provided before the release can occur.

Foreign Governments and Officials

4. The release of classified information to foreign governments, foreign individuals and other foreign entities is to be completed in accordance with DSPF Principle 15 - *Foreign Release of Official Information*.

Intra-Government Presentations

5. Presentations at which only appropriately cleared Australian Government employees and integrated officers are present do not constitute public release. The presenter is to:

a. confirm that the security clearances and nationalities of the audience are appropriate;

b. confirm that the physical security and IT accreditation of the facility are appropriate;

c. inform the audience of the classification level of the information being disclosed; and

d. remind the audience of its obligation under the PSPF to protect the information.

Public Release

6. Public release of Official Information is to be done in accordance with the Defence Communication Manual, Chapter 2 – *Media Engagement and Public Comment*.

7. Where Official Information is intended for public release or publication, it may have confidentiality requirements before release (for example, Budget papers.) In these instances, when applying Protective Markings, the originator is to indicate when the information is to be released to the public and the Protective Markings removed.

Freedom of Information

8. The release of Official Information in response to a freedom of information request is to be completed in accordance with the *Freedom of Information Act 1982* (*the FOI Act*). For advice, contact the Freedom of Information Directorate.

***Note**: The FOI Act has exemptions from disclosure for Official Information affecting national security, Defence or international relations. It also has an exemption for information communicated in confidence by a foreign government. This includes information communicated pursuant to any agreement or other formal instrument on the reciprocal protection of classified information, such as Security of Information Agreements and Arrangements.*

Release to Industry

9. Unclassified Official Information covered by a DLM (Sensitive and FOUO) may be released to Contractors, Consultants and Outsourced Service Providers subject to the need-to-know principle.

10. Industry accessing this information may require Defence Industry Security Program (DISP) membership. DISP membership for access to information at this level is not mandatory but may be required, subject to a security risk assessment. For further information refer to DSPF Principle 16 - *Defence Industry Security Program*.

11. Industry accessing this information may require their ICT systems to be accredited to the ISM Government standard in order to process this information electronically. Accreditation requirements for ISM G level systems are undertaken

based on an assessment of risk. For further information see DSPF Principle 23 - *ICT Certification and Accreditation*.

12. Official Information classified PROTECTED and above is only to be released to DISP members which have:

a. staff cleared to the required level of access;

b. accredited facilities to store the material; and

c. (if electronic access is necessary), accredited ICT systems to process the material.

***Exclusion**: PROTECTED material in hardcopy form may be released in limited quantities to non-DISP members and other individuals that do not hold a security clearance. Refer to DSPF Principle 41 - Temporary Access to Classified Information and Assets for release criteria that apply to access to PROTECTED material without a RESTRICTED or BASELINE security clearance.*

State, Territory and Local Governments

13. The release of classified information to State, Territory and local government departments and agencies, or any agency not bound by the PSPF, **must** have the written approval of the owner or originator of the information who **must** hold a position at or above the EL2 / O-6 level. For further advice, contact the Defence Security and Vetting Service (DS&VS) Regional Office or the Executive Security Authority.

Courts

14. Where documents sought under a court order are classified, the Subpoena Clerk in the Directorate of Litigation (DLIT) is to be contacted as soon as possible. The Subpoena Clerk will seek advice from a Legal Officer in the DLIT and consult DS&VS about the release of the documents.

Parliamentary Committees

15. All Defence involvement in Parliamentary Committees requires approval from the Minister for Defence. For further information refer to the Ministerial and Parliamentary Branch.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Release of Official Information
Annex Version	2
Annex Publication date	31 May 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Classification and Protection of Official Information
DSPF Number	Control 10.1

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 SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex E to Classification and Protection of Official Information – Registration of Protectively Marked Information

1. All information classified TOP SECRET, and accountable material, held by Defence **must** be registered. Information at other classifications held by Defence should be registered.

2. All information classified SECRET and above, and accountable material, held by Defence Industry Security Program members **must** be registered. Information at other classification held by Defence Industry Security Program members should be registered.

3. When manual methods are required for classified document recording, Form XC040 – Classified Document Register (Defence) (CDR) is to be used. Defence Industry Security Program (DISP) members use Form AC458 – Classified Document Register (Industry).

Note: *CDRs are to be classified on their merits and not according to the security classification of the documents they record, unless the title of the document itself is security classified. In this instance, it is suggested that the originator create a separate UNCLASSIFIED reference title. With due care, the CDR should rarely need to be classified. Where the volume of correspondence justifies it, separate registers for each classification and inwards and outwards correspondence may be used.*

4. The Objective application offers electronic registration and auditing features which are compliant with the *Archives Act 1983* and meet some of the registration requirements of the DSPF. The following instructions apply to the use of the Objective application:

a. Codeword information **must not** be stored in Objective on either the Defence Restricted Network (DRN) or Defence Secret Network (DSN).

b. Where a classified document is created as an electronic document within Objective there is no requirement to register that document into a CDR. Classified documents created in Objective are not to be placed on hard copy files, instead they should be stored on Objective virtual or mixed mode file.

c. When converting a physical record to a digital record it is necessary to ensure that the new digital record remains authentic, reliable, integral and

usable. The integrity of the record is to remain protected, complete and unaltered by the digitisation process. When original source records are digitised they are to inherit the access, destruction or transfer arrangements applicable to the original physical record. For further information, refer to the Records Management Manual (RECMAN).

d. The preferred method of distributing documents is by sending an Objective link. When a document classified CONFIDENTIAL or above is printed from Objective for manual distribution, the document is to include the Object ID.

e. A CDR entry is required to track dispatch and return receipt of the physical document via Form XC051 - *Dispatch Advice/Receipt for Classified Matter*. For further information on the requirements for the physical transfer of classified information refer to DSPF Principle 71 - *Physical Transfer of Information and Assets*.

5. TOP SECRET information is to be registered in a separate Form XC040 or Form AC458 as applicable. It is recommended that access to TOP SECRET registers is limited to individuals with a demonstrated need-to-know for the subject matter and for the extent of TOP SECRET holdings of a particular military or business unit.

6. **Registration of hard copy draft or working papers.** Material that is accountable or classified TOP SECRET **must** be registered in a CDR when:

a. completed as a finished document; or

b. retained for more than seven days after creation, regardless of the stage of development.

7. Classified hard copy draft or working papers are to be:

a. dated when created;

b. marked with their overall classification, and with the annotation ‘Draft’ or ‘Working Paper’; and

c. destroyed when no longer needed.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Registration of Protectively Marked Information
Annex Version	2
Annex Publication date	31 May 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Classification and Protection of Official Information
DSPF Number	Control 10.1

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 SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex F to Classification and Protection of Official Information – Official Information Filing and File Census

1. Official Information is to be filed in accordance with the *Archives Act 1983* and the Records Management Policy Manual (RECMAN).

2. A file **must** carry, as a minimum, the Protective Marking of the highest level of security classified information it holds. When new information is added to the file, the file user is to ensure that the classification carried by the file is still appropriate. If the information to be added is at a higher classification than the file itself, the file user is to reclassify the file before attaching the new document.

Note: *Active files that are protectively marked with former security classifications and X-in-Confidence markings are to be remarked with the equivalent current security classification Protective Markings. Refer to this DSPF Control for further information on equivalences.*

3. Security classified Official Information that can be filed is to be placed on an appropriate file as soon as possible after its creation or receipt (usually following registration in a classified document register).

File Types

4. It is essential that the classification of the file be clearly and easily identifiable and easily distinguished from other classifications. The standard colour file covers for security classified files are:

a. TOP SECRET – post office red;

b. SECRET – salmon pink;

c. CONFIDENTIAL – green;

d. PROTECTED – (formerly: green plus stripe. Post 1 Oct 2018 PSPF revision, blue); and

e. DLM (FOUO, Sensitive) – blue, buff, blue plus stripe, buff plus stripe.

i. Former RESRTICTED and X-in-Confidence file covers may continue to be used, over stamp the former protective marking with the new AGSCS marking and reclassify the file in the appropriate records management system.

***Note**: The recommended file stripe colour is Pantone Process Yellow-2U. The stripe is to run diagonally across the front and on the spine.*

Filing Procedures

5. The normal filing procedures such as file reference and folio numbering can be used for security classified files to maintain a record of the information held on the file. It is also good practice to follow normal filing procedures such as recording the date and name of the person holding the file from time to time.

6. It is recommended all Defence files have a folio sheet placed in the inside front cover of the file. An example of a folio sheet is provided at Table 1 of this DSPF Annex.

7. If a folio sheet is used, it is recommended all files have the documents within the file folio numbered sequentially.

Table 1 – Example of Folio Sheet

FILE TITLE:

FILE NUMBER: _____

Folio	Date	Sender / Originator	Doc Type	Subject	Class	CDR

File Census

8. A file census of information classified CONFIDENTIAL, SECRET, or TOP SECRET, and Accountable Material is to be conducted at least every two years. At the discretion of the Commander or Manager, it is recommended that a file census occurs:

a. annually, if substantial file holdings exist in the unit of facility;

b. when the Security Officer or document custodian changes; and

c. if a security incident or suspected compromise of a file occurs.

How to Conduct a File Census:

9. The Security Officer conducts or coordinates the census on behalf of the Commander or Manager. The local procedure for the census is recorded in the unit or facility Security Standing Orders.

10. All files are to have their documents checked against the folio sheet. Details of any missing documents are to be retrieved from the folio sheet and, if applicable, from the classified document register. Action to be taken as a result of missing documents is detailed in DSPF Principle 77 - *Security Incidents and Investigations*.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Official Information Filing and File Census
Annex Version	2
Annex Publication date	31 May 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Classification and Protection of Official Information
DSPF Number	Control 10.1

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 SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.

Defence Security Principles Framework (DSPF)

Annex G to Classification and Protection of Official Information – Copying and Reproduction of Protectively Marked Information

Copying and Reproduction

Copying and Reproduction

1. To help reduce the risk of compromise, copying and reproducing protectively marked Official Information is to be done only when it is necessary. Spare or spoilt copies of protectively marked Official Information are to be destroyed immediately. Refer to Annex H of this DSPF Control for further information on disposal and destruction methods. This destruction is defined as 'normal administrative practice' in terms of the *Archives Act 1983* and does not need specific permission from the National Archives of Australia.

Note: *The scanning of documents into Objective for filing is an administrative procedure and does not constitute copying or reproduction. Refer to Annex F of this DSPF Control for further information on scanning documents into Objective.*

2. For information classified CONFIDENTIAL and above, details of copies and reproductions are to be included in a Form XC040 Classified Document Register (Defence) (CDR). In the case of TOP SECRET and Accountable Material, each original document and reproduced copy is to be numbered. Any additional protective measures imposed by the originating authority are to be strictly observed. Persons authorising the copying of TOP SECRET information are to record in the file bearing the original the details of the number of copies made and their distribution.

3. Accountable Material **must not** be copied or reproduced by anyone other than the originator. If extra copies of such documents are required, additional copies are to be requested from the originator. Information **must not** to be extracted from Accountable Material without the permission of the originator.

Exclusion: *exemptions exist for source codeword and some other Accountable Material when being handled within an originating intelligence agency's premises. Intelligence agency staff are to refer to their agencies' document handling procedures for further information on the operation of exclusions to this policy within their agency.*

Use of Multi-Function Devices

4. Most current multi-function devices (MFD) incorporate data storage capabilities in the form of non-volatile memory such as hard disks or flash memory. Combined with communication and data transfer capabilities, MFD are effectively ICT systems.

5. Any entity providing MFD including photocopiers, printers, facsimile machines and similar devices, **must** treat these as part of the ICT system to which they are connected, with security addressed in accordance with DSPF Principle 20 - *Information Systems Lifecycle Management*.

Example: *A multi-function printer / photocopier device connected to the DRN is to be considered as part of the DRN and be managed from a security perspective in accordance with DSPF Principle 20 - Information Systems Lifecycle Management.*

6. Any MFD that are not connected to a larger ICT system or network **must** be treated as ICT systems in their own right, with security addressed in accordance with DSPF Principle 20 - *Information Systems Lifecycle Management*.

Note: *A collection of independent MFD may be certified and accredited as a fleet and covered by a single set of security documentation.*

7. Standard Operating Procedures (SOP) covering the use of MFD **must** be available to users.

8. MFD **must** be used in accordance with the applicable SOP.

Commercial Printing

9. If a commercial printing service is considered for the copying or reproduction of Official Information not intended for public release then it may be required to be a member of the Defence Industry Security Program (DISP), depending on the volume and type of information. For further information on considerations by Commanders or Managers in this regard refer to DSPF Principle 16 - *Defence Industry Security Program*.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Copying and Reproduction of Protectively Marked Information
Annex Version	2
Annex Publication date	31 May 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Classification and Protection of Official Information
DSPF Number	Control 10.1

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 SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex H to Classification and Protection of Official Information – Disposal and Destruction of Protectively Marked Information and Assets

1. Disposal of any Commonwealth record is to be done in accordance with the *Archives Act 1983* (the Act). Under the Act it is illegal to destroy Commonwealth records without the permission of the National Archives of Australia (NAA), or in accordance with a practice or procedure approved by the NAA, unless the destruction is required by law.

Note: *For Defence policy refer to the Records Management Policy Manual (RECMAN).*

Disposal and Destruction Procedures

2. When TOP SECRET information and assets or Accountable Material need to be destroyed, the destruction **must** be conducted under the supervision of two persons who are security cleared to at least the classification of the information or asset being destroyed.

Recording Disposal and Destruction

3. Details of the disposal of all classified documents or assets recorded in the Classified Document Register (CDR) are to be clearly annotated alongside each individual document record and those carrying out the destruction are to sign the CDR or document register.

4. The originator of a copy-numbered classified document **must** be consulted prior to the destruction of such a document. If the originator approves destruction of the copy-numbered document, the destruction is to also be recorded by completing Form XC024 - Certificate of Destruction for Classified Material. The completed Form XC024 is then to be sent to the document originator.

5. For as long as any one document recorded in a given CDR is still in existence, the CDR is to be maintained. Following destruction of the final document recorded in a CDR, the CDR is to be retained for at least five years before being destroyed in accordance with RECMAN.

6. The book of Form XC051 - Dispatch Advice/Receipt for Classified Matter **must** be retained for at least five years after the last Form XC051 is returned. For information regarding CDR, refer to the DSPF Principle 71 - *Physical Transfer of Information and Assets*.

7. **Sensitive: Cabinet.** Information which bears the DLM Sensitive: Cabinet is to be disposed of in accordance with the practices mandated by the Department of the Prime Minister and Cabinet. Refer to the Cabinet Handbook.

8. **High grade cryptography and communications security.** High grade cryptography and communications security (COMSEC) material is to be handled in accordance with the DSPF and its authoritative sources.

9. **Electronic media.** Electronic media is sanitised/destroyed in accordance with the requirements of the Information Security Manual (ISM).

Shredders

10. Shredders used to destroy paper-based classified information are to be compliant with the requirements found in the current ASIO Security Equipment Guide (SEG)-01 *Class A and B Paper Shredders*.

11. Shredders used to destroy ICT media containing classified information are to be compliant with the requirements found in the current ASIO SEG-09 *Optical Media Shredders*.

Note: *Commercial strip shredders are not suitable for the destruction of classified or sensitive information. The smaller the particle size the more secure the results.*

Destructors

12. Destructors (disintegrators and hammermills) used to destroy both paper-based and ICT media containing classified information are to be compliant with the requirements found in the current ASIO SEG-18 *Destructors*.

Garbage and Recycling

13. Protectively marked information is not to be disposed of by garbage or unsecure recycling collection unless it has already been through one of the above approved destruction processes.

14. Garbage, whether it is placed in a garbage hopper or other area for collection or delivered directly to a garbage disposal service, is extremely vulnerable. Only information that is public domain information or has already undergone an approved destruction process, such as shredding, may be discarded in Defence general garbage.

15. Recycling or discarding intact documents does not serve the same purpose as document destruction and can only be used for public domain information disposal or when information has already undergone some form of appropriate destruction, such as shredding.

Contracted Disposal and Destruction

16. It may be considered necessary, after a comprehensive risk assessment, for the disposal of security classified waste to be undertaken by an authorised disposal company. Requirements can be found in ASIO Protective Security Circular 167 – External Destruction of Security Classified Information.

17. The destruction of TOP SECRET or Accountable information or assets is to occur within a Defence facility. The originator of the information may also apply special conditions to the destruction of some classified information which might prohibit the use of contractors. Form XC024 - Certificate of Destruction for Classified Material, is to be sent to the originator upon destruction of the material.

18. Classified waste bags are used to temporarily store classified waste until a contractor can carry out complete destruction. Classified waste bags **must** be stored according to the highest level of classification of their contents.

Destruction of Classified Information Overseas

19. Where possible, classified information or assets located overseas are to be transferred to an Australian controlled area, such as an Australian Embassy or High Commission, for destruction if appropriate transportation for the classified information or asset back to Australia cannot be arranged.

Note: *Classified information and assets created or transferred overseas must be handled in accordance with DSPF Control 71.1 - Physical Transfer of Information and Assets.*

Emergency Destruction Plan

20. Defence units are sometimes in sensitive areas where there is a risk of uninvited entry by unfriendly forces. In such cases, Commanders of Defence units in sensitive areas **must** develop an emergency destruction plan. The Commander should appoint a Security Officer, or an appropriate officer in the unit, to be responsible for keeping the emergency destruction plan current.

21. The emergency destruction plan is to:

a. identify the order and method of destruction of all classified documents and information embedded in electronic systems; and

b. ensure that the most highly classified and sensitive information or assets are destroyed first should the complete destruction of all classified information be necessary.

22. If Security Standing Orders are applicable to a unit on deployment, the plan is to be incorporated into those orders.

23. **Aircraft.** Contingent Commanders who have aircraft making flights over foreign territories **must** develop:

a. a list of security classified information or assets carried on each type of aircraft; and

b. a plan detailing the order and method of destruction of each classified item.

Additional Requirements for Classified Assets

24. Classified assets **must** be destroyed so that:

a. the security nature of the asset cannot be identified;

b. security classified performance details or data cannot be recovered;

c. components, if not totally destroyed, are no longer operational; and

d. the relationship of components to the overall asset cannot be identified.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Disposal and Destruction of Protectively Marked Information and Assets
Annex Version	2
Annex Publication date	31 May 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Classification and Protection of Official Information
DSPF Number	Control 10.1

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 SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.

Defence Security Principles Framework (DSPF)

Annex I to Classification and Protection of Official Information – Remarking Information Bearing Former Security Classifications

1. On 1 October 2018, the Attorney-General's Department released a new version of the Protective Security Policy Framework that included a revised system of Protective Markings for classified information and assets. The revised system of Protective Markings effectively replaces the Australian Government Security Classification System (AGSCS). Defence is required to fully implement the revised Protective Markings by 1 October 2020.

2. Defence will continue to use the former AGSCS until it implements the revised Protective Markings by 1 October 2020. However, it is important to note that there are legacy security classifications (Protective Markings) in circulation that predate the introduction of the AGSCS and still require instruction on their handling and storage.

Former Security Classifications

3. On 31 July 2014, some security classifications were phased out and replaced with AGSCS equivalents; the following paragraphs detail grandfathering arrangements for Protective Markings that pre-date introduction of the AGSCS.

4. Since 31 July 2014, the former security classification HIGHLY PROTECTED cannot be used on active Defence records. Records reused since this date are to be remarked SECRET. Records and documents that are inactive or archived do not require remarking unless they are reused. Inactive and archived records are protected as for SECRET material.

5. Since 31 July 2014, the former security classification of RESTRICTED cannot be used on active Defence records. Records reused since this date are to be remarked using the DLM ‘For Official Use Only' (FOUO). Records and documents that are inactive or archived do not require remarking unless they are reused. Inactive and archived records are protected as for FOUO material.

6. The remarking of documents from former classifications to AGSCS equivalents does not require the permission of the document’s originator. However

any caveats such as CODEWORD or release markings cannot be modified under these provisions.

Former X-in-Confidence Markings

7. Under the PSPF, all X-in-Confidence markings have been phased out and replaced with equivalent AGSCS protective markings. The following paragraphs detail grandfathering arrangements for these markings.

8. The former X-in-Confidence markings cannot be used on active Defence records after 31 July 2014. Records that are reused after this date are to be remarked with their equivalent AGSCS protective marking.

9. Records and documents that are inactive or archived do not require remarking unless they are reused. Inactive and archived records are protected in accordance with any assigned classification, or in the case of UNCLASSIFIED information as per DLM marked material.

10. X-in-Confidence material is to be remarked in accordance with Table 1.

Exclusion: *if the information marked 'Audit-in-Confidence' or 'Security-in-Confidence' contains personal information it is to be marked with 'Sensitive: Personal'.*

11. Former X-in-Confidence markings that are not included in Table 1 are to be assessed against the AGSCS DLM criteria and have the appropriate DLM applied.

12. Remarking of documents from former X-in-Confidence markings to the equivalent AGSCS DLM does not require the permission of the originator. However any caveats such as CODEWORD or release markings cannot be modified under these provisions.

Table 1 – Mapping of former X-in-Confidence Markings to AGSCS Equivalents

Former Marking	AGSCS Dissemination Limiting Marker (DLM)
• Commercial-in-Confidence • Audit-in-Confidence • Security-in-Confidence • Committee-in-Confidence	• For Official Use Only
• Cabinet-in-Confidence	• Sensitive:Cabinet
• Legal-in-Confidence	• Sensitive:Legal
• Medical-in-Confidence. • Psychology-in-Confidence • Client-in-Confidence • Staff-in-Confidence • Honours-in-Confidence • Audit-in-Confidence* • Security-in-Confidence* * Only when personal information is collected	• Sensitive:Personal

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Remarking Information Bearing Former Security Classifications
Annex Version	2
Annex Publication date	31 May 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Classification and Protection of Official Information
DSPF Number	Control 10.1

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 SPS	Launch
2	31 May 2019	AS SPS	Foundational review; PSPF update; and security classification alignment.

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex J to Classification and Protection of Official Information – Creating and Managing Information Compartments

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this Enterprise-wide Control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control is For Official Use Only and has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Creating and Managing Information Compartments
Annex Version	1
Annex Publication date	31 May 2019
Releasable to	Defence
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Classification and Protection of Official Information
DSPF Number	Control 10.1

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	31 May 2019	AS SPS	Created to consolidate PROTECTED content.

Defence Security Principles Framework (DSPF)

Security for Projects

General principle

1. Projects of a type referred to in the Expected Outcomes below, and Integrated Project Teams (IPTs) need to incorporate security planning into project activities and all stages of the Capability Life Cycle. Security is to be maintained throughout the planning and execution of all projects. Planning is to incorporate the expenditure required to deliver appropriate security measures.

Rationale

2. Projects and IPTs carry significant security responsibilities. Failure to adequately protect official information and any capability that is acquired or supported, both during the project phase and on the introduction into service of any new capability, has security and financial consequences for Defence. Failure to consider and forecast security requirements throughout the capability's lifecycle, including assessing the security impacts on all Fundamental Inputs to Capability (FIC) elements, could lead to:

a. project delays;

b. increased security risks;

c. security compromised capabilities;

d. systematic security failings between Support Organisations and Project/Capability Managers; and

e. increased costs due to remediation activities.

Expected outcomes

3. Security planning is undertaken for all projects that involve:

a. acquisitions conducted under the Defence Integrated Investment Program;

b. the establishment, or major renovations, of the Defence estate or facilities infrastructure;

c. collaborative engagements between industry or allies (e.g. joint ventures, outsourcing, or research and development.); or

d. some aspect(s) requiring consideration to be given to security matters.

4. Compliance with security policy is maintained during project planning and execution stages, and throughout all phases of the Capability Life Cycle.

Note: *Although projects are unlikely to run for the full duration of a capability's life cycle they should consider the security implications of as many phases of it as appropriate in the circumstances.*

5. Adequate risk mitigation strategies are in place.

6. Security costs and accountabilities are included in the project design and delivery.

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 Program Management (ASPM)
High	Defence Security Committee (DSC) – through ASPM
Extreme	DSC – through ASPM

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Security for Projects
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	PRINCIPLE 11
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 11.1
Control Owner	Assistant Secretary Program Management (ASPM)

Related information

Government Compliance	**PSPF Core Requirements:** Security Planning; Security governance for contracted service providers; and Eligibility and suitability of personnel. **Legislation:** *Workplace Health and Safety Act 2011* (Cth)
Read in conjunction with	Interim Capability Life Cycle Manual Estimates Memorandum 2015/51 – Defence Specific Costing Requirements for Projects in the Defence Integrated Investment Programme.
See also DSPF Principle(s)	Security for Capability Planning
Implementation Notes, Resources and Tools	Australian Government physical security management protocol: https://www.protectivesecurity.gov.au/physicalsecurity/Pages/Protocol.aspx Security Equipment Guides (SEGs) via the Security Toolkit. ASIO Tech Notes via the Security Toolkit. Security Equipment Evaluated Product List (SEEPL). This list contains products endorsed by the Security Construction and Equipment Committee (SCEC). Contact the Protective Security Advice Centre PSAC or your Service Security Adviser (SSA). The Defence Industry Security Program.

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

Defence Security Principles Framework (DSPF)

Security for Projects

Control Owner

1. The Assistant Secretary Program Management (ASPM) is the Control Owner for this control under the Administration & Governance Domain of the administrative policy framework (which includes security). The Associate Secretary is the Accountable Officer for this domain. The First Assistant Secretary Security and Vetting Service (FAS S&VS) is the Policy Owner for security.

2. The ASPM is also the Policy Owner for Project management under the Acquisition & Sustainment domain. The Deputy Secretary, Capability Acquisition & Sustainment Group (DEPSEC CASG) is the relevant accountable officer. The ASPM is also the Program Management Centre of Expertise Lead as defined in the CASG Business Framework.

Framework Escalation Thresholds

3. The ASPM has set the following general threshold 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	ASPM
High	Defence Security Committee (DSC) – through ASPM
Extreme	DSC – through ASPM

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Controls

Project Security Planning

4. On appointment of an interim Integrated Project Management Team under the Capability Life Cycle, the Project security planning process is used to identify and document the relevant security authorities, standards, specifications, procedures and practices necessary to comply with Defence security policy during the Project. The Project security planning process should gather information from, and be a continuation of any previous security planning.

5. This process is based on a risk management approach, and is maintained throughout the Project's life. A security plan for the Project is developed from the following process:

a. for major capital Projects, security risk will be recorded in the Project's risk register in accordance with business processes for managing Project risk; or

b. for smaller Projects, security risks can be recorded in a separate register.

6. The security planning processes are recommended for all other Defence capability proposals and Projects

Project Security Function

7. Projects are to consider the need for the appointment of a Security Manager.

8. In addition to a Security Manager, an Integrated Project Management Team is to be responsible for the Project security function for major capital Projects, infrastructure Projects involving new Defence facilities and major renovations to the Defence estate. This function should also be established for minor capital and collaborative Projects.

9. The composition of Integrated Project Management Team members will depend on the Project. Membership may comprise representation from:

a. the Project Owner / Project Sponsor;

b. the Executive Security Authority (ESA);

c. Chief Information Officer Group (COMSEC and Defence Information Environment architects);

d. ICT and physical certification and accreditation authorities;

e. business process owners and those who share Project security risk;

f. the Defence Estate and Infrastructure Group, particularly where there are extensive changes to the Defence estate;

g. the Base Support Manager or Senior Australian Defence Force Officer (SADFO) at bases that house related facilities and assets; and

h. contractor(s), when selected.

10. The Project security function should advise the Integrated Project Manager and Project Sponsor on security matters such as:

a. developing and approving Project Security Instructions (PSI) that meet stakeholders' needs;

b. coordinating concurrent security activities across multiple Projects and areas;

c. identifying security risks and treatments;

d. identifying security costs, including security costs and resources that will be required of areas outside Project managers control; and

e. engaging with accreditation authorities.

Project Planning

11. Project security costs are to be identified and resourced throughout all stages of the planning for and execution of a Project (refer to Estimates Memorandum 2015/51 – Defence Specific Costing Requirements for Projects in the Defence Integrated Investment Program.) Security costs are to be identified for all Fundamental Inputs to Capability (FIC) through all stages of the Capability Life Cycle. Considering these costs early in Project planning allows for more accurate costing and scheduling of important Project security activity, including, but not limited to:

a. Project Office and contractor security arrangements, including:

   i. gaining facility or ICT system accreditation; and

   ii. identifying the requirement for staff or external service providers to obtain personnel security clearances or DISP membership as appropriate (refer DSPF Principle 16 - *Defence Industry Security Program*); and

b. asset and Capability security lifecycle costs, including:

   i. in service security costs such as additional security clearances, physical security infrastructure and enhanced guarding requirements on introduction to service; and

ii. disposal costs such as the destruction of security classified equipment or sanitisation of ICT resources prior to resale or disposal.

Project Security Reviews

12. Project security reviews are to be conducted throughout the Project. The purpose of a Project security review is to confirm that security documentation is current and that all security risks are identified and appropriately treated. Regardless of the size or complexity of a Project, the Project's security related documentation should be updated regularly so that it is relevant to the Project's activities.

13. For capital and intelligence Projects, the Integrated Project Manager should conduct Project security reviews at least annually, and to inform Capability Life Cycle stages and processes including but not limited to:

a. Decision making forums convened by Program Steering Groups;

b. Health Checks;

c. Independent Assurance and In-Depth reviews;

d. Before Gate approvals;

e. During the Risk Mitigation and Requirements Setting Phase if Capability risk mitigation activities are being held, for example, a major trial;

f. Prior to tender documentation being released;

g. On acceptance of the preferred solution in order to identify any security implications of the preferred solution, including costing of security impacts, in preparation for contract negotiations;

h. During the Acquisition Phase in order to ensure the implementation of agreed security measures by the Integrated Project Manager and external service providers;

i. Immediately prior to the transition into service in order to ensure that Capability owners have adequate security in place to take delivery; or

j. Prior to disposal to ensure the secure disposal of classified resources and the return of all official information and assets from external service providers.

14. For research and Projects other than major or minor capital Projects and intelligence Projects, the Project Managers:

a. should conduct a Project security review of security risks and relevant Project documentation prior to Project approval in order to:

i. confirm compliance with security policy;

ii. ensure adequate risk mitigation strategies are in place; and

iii. confirm that security costs have been included in the Project design and delivery.

b. should conduct Project security reviews at least annually after Project approval.

Note: *It is recommended that Integrated Project Managers observe the schedule above at the equivalent phases of the Project.*

Note: *For smaller Projects not included above, a Project security review may entail the development of a series of exploratory questions to determine appropriate levels of security preparedness. Exploratory questions could include - is classified infrastructure required? Are there enough security cleared staff available? Does the Project have the room to store all of the documents it will be producing?*

Security Activities by Capability Life Cycle Phase

Strategy and Concepts Phase

15. A security risk assessment should be conducted during the development of the Gate 0 Business Case and be documented as part of the Integrated Project Management Plan in order to ensure that security costs are included in the design planning for the Project and the introduction into service of the planned Capability.

16. During this phase, the following security aspects should be addressed:

a. classification of the existence of the Project;

b. security of Project management activities;

c. identification of the Project;

d. who is involved;

e. where and how the Project will be managed and/or developed;

f. the requirement for secure communications Capability between Project stakeholders;

g. schedule of security related activities such as accreditation of facilities and ICT systems; and

h. the security of the Capability to be acquired, including transition into service, in-service support and disposal.

Note: *This information may start out generically and be tailored as the Project moves towards later acquisition phases.*

17. For all major and minor Projects, and based on a risk assessment, the Integrated Project Manager (or Project Sponsor or Project Director if no Project Manager has been appointed), should provide to the Defence Security and Vetting Service (DS&VS) the following security documents for approval:

a. Project Identification Document (PID) - refer to the recommended format on the Defence Security Portal

b. Security Classification and Categorisation Guide (SCCG) – refer to the recommended format in DS&VS Security Operations – Projects; and

Note: *Projects acquiring assets with an existing Security Classification Guide provided by the vendor nation may incorporate it into the Australian SCCG as an annex. The DS&VS is to be consulted in this instance.*

c. Program/Project Security Instruction – The PSI Template should be completed for any projects with an Australian Resident project team overseas, or that operate under a Bilateral or Multinational Cooperative Defence Program or Project Arrangement. Security Standing Orders otherwise apply.

Note: *These documents are to be provided to DSA.ProjectSecurity@defence.gov.au at the earliest possible stage of the project.*

18. For Defence intelligence agencies' projects, the documents listed above should be approved by the Deputy Secretary Strategic Policy and Intelligence, the head of the relevant intelligence agency or its senior management committee.

19. Integrated Project Managers are to contact the DS&VS for advice regarding projects with overseas components to ensure compliance with any international obligations.

20. Where the project has staff located overseas (such as when staff are part of a Resident project team), and based on a risk assessment, a separate PSI covering the overseas components should be produced using the template on the Defence Security Portal.

21. Security classifications and Business Impact Levels (BILs) are applied to the systems, sub-systems, components and project information via the SCCG. The

measures required to protect the information and assets are then identified and documented in the PSI.

22. Research projects, and projects other than capital and intelligence projects, are not required to submit any of the above documentation to the DS&VS; however, the Project Manager should develop a SCCG if the project involves:

a. a significant scientific breakthrough with implications for national security;

b. a designated high technology area of research; or

c. commercial sensitivities, including:

   i. a development unique to Australia that might have marketing potential;

   ii. individuals or organisations outside of Defence, such as academic or commercial research and development specialists; and

   iii. a patent application.

23. Integrated Project Managers are responsible for the production of security documentation. The DS&VS can provide assistance in their development.

Risk Mitigation and Requirements Setting Phase

24. During this phase the following security aspects are considered:

a. trials and risk mitigation activities;

b. tendering and tender response activities (including security requirements related to the release of project-specific official and classified information); and

c. where multiple Capability solutions are being compared, security aspects are considered for each solution:

   i. solution specific risks, including Capability risks and any shared risks introduced by a proposed solution; and

   ii. associated security costs.

25. Where a project involves trials and testing, a security plan covering these elements should be developed.

26. Where testing of equipment is conducted, the classification of information in relation to the performance of equipment should be reviewed after the activity has occurred. This is necessary as the actual performance of the activity may differ to that anticipated at the beginning of the project and could impact the classification level.

27. If changes are made during negotiations, the PID should be resubmitted to the DS&VS before contract signature.

Acquisition Phase

28. DSPF Principle 82 - *Procurement* addresses many security issues that projects will encounter during the acquisition phase. Immediately prior to the transition into service phase, the scheduled security review should be conducted. The focus of this review is to ensure that Capability owners have adequate security in place to take delivery. It is important that SCCGs are reviewed prior to the introduction into service as this document will be used by the recipients of the Capability to determine security for the delivered solution.

29. During the transition into service phase, Integrated Project Managers are to monitor and review the security aspects of in-service support and, in conjunction with the Capability Users, regularly review SCCGs to ensure adequate protection measures remain in place.

In-Service and Disposal Phase

30. During the in-service phase, the project office will either assume responsibility for logistics security and maintenance security of the delivered Capability, or the project will be complete. Security procedures for the logistics security and maintenance security functions will require regular review to ensure that they remain effective.

31. Immediately prior to the disposal or project closure phase, the scheduled security review should be conducted. The focus of this review is to ensure that classified material, including both assets and information, is correctly disposed of. Issues to consider are:

a. security-protected assets are transferred, sanitised or destroyed as appropriate;

b. appropriate security arrangements, including disposal arrangements for security-protected assets and classified information, are accepted by the Capability Manager responsible for the in-service operation of the delivered Capability;

c. the project's official and classified information is archived; and

d. External service providers associated with the project have returned all official information to Defence or have destroyed it.

32. During disposal, the Project Manager will monitor the disposal and transfer of information and security protected assets.

33. During project closure, Integrated Project Managers should:

a. review the project's security performance and provide a report to the DS&VS, noting any outstanding security issues as well as any lessons learnt during the conduct of the Project; and

b. confirm that in-service support agencies have appropriate security arrangements in place to enable compliance with applicable parts of the DSPF.

Roles and Responsibilities

First Assistant Secretary Security and Vetting Service

34. FAS S&VS is responsible for:

a. providing protective security advice to Integrated Project Managers and Security Officers; and

b. approving PSIs to ensure that all project security requirements have been adequately considered and addressed in the circumstances that Security Standing Orders do not apply.

Capability Managers, Delivery Groups and Enabler Groups

35. Capability Managers, and delivery and enabler Group Heads are responsible for the security of all projects managed by their respective Groups and Services and for the appointment of the Project Managers responsible for a project's security. This responsibility may be delegated by Capability Managers to Program Sponsors and by delivery and enabler Group Heads to Program Managers.

Chief Defence Scientist

36. The Chief Defence Scientist (CDS) is responsible for the development of security policies and procedures to be applied to protect the research programs and associated collaborative activities undertaken by Defence Science and Technology Group (DST Group).

Chief Information Officer

37. The Chief Information Officer (CIO) is, where appropriate, responsible for:

a. providing ICT and Communications Security (COMSEC) advice to Project Managers and Security Officers; and

b. reviewing SCCGs and PSIs to ensure that all ICT security and COMSEC recommendations have been adequately considered and addressed.

Program Sponsor

38. The Project Sponsor is accountable to the Capability Manager through the Program Sponsor for the management of security within the Project.

Program Manager

39. The Program Manager is responsible for the management of security of all projects within their Program and is responsible for the appointment of an Integrated Project Manager.

Project Sponsor

40. The Project Sponsor is accountable to the Capability Manager through the Program Sponsor for the management of security within the Project.

Integrated Project Manager

41. The Project Manager is responsible for:

a. the security of all aspects of the project, including managing the security risk associated with the project;

Note: *external service providers, including Defence Industry Security Program (DISP) members, cannot accept security risks on behalf of the Commonwealth. Therefore, if DISP members or other external service providers are engaged, the Project Manager, via their contract manager, retains responsibility for managing all outsourced risks.*

b. ensuring that protective security requirements are considered and budgeted for throughout the project, including the consideration of security requirements associated with the Capability to be delivered by the project prior to its introduction into service;

Note: *where a project is acquiring assets or building infrastructure, the Project Manager is responsible for security requirements planning and any related expenditure throughout the entire lifecycle of the assets or building infrastructure.*

c. advising the DS&VS of the nature of larger projects and anticipated security impacts to facilitate the provision of advice to Project Managers and Security Officers by DS&VS ;

d. advising CIOG of the nature of larger projects (with significant ICT infrastructure or accreditation requirements), and description of the ICT and COMSEC aspects of the project so that CIOG may provide advice to Project Managers and Security Officers;

e. appointing a project Security Officer for large or sensitive projects;

f. ensuring that facilities and ICT systems used by the project to store, process or communicate official or classified information or material are accredited prior to use in accordance with DSPF Principle 23 - *ICT Certification and Accreditation* and DSPF Principle 73 – *Physical Security Certification and Accreditation*;

g. ensuring that appropriate security classification guidance is available to all Defence personnel, Contractors, Consultants and Outsourced Service Providers associated with the project. To ensure proper coordination of all security matters within a project, the Project Manager is to determine the relevant Group or Executive Security Adviser for the project;

h. ensuring compliance with Defence security policy within their project; and

i. reviewing all security documentation, appointments and arrangements to ensure the ongoing security of the project, prior to commencement of the project.

Security Officer

42. Security Officers may assist their Project Manager with the necessary administrative actions to enable compliance with this DSPF part. This may include providing the Integrated Project Manager with security advice and support related to:

a. the development, maintenance and review of Project security documentation;

b. the determination of the Project's ICT and physical accreditation requirements, refer to DSPF Principle 23 - *ICT Certification and Accreditation* and DSPF Principle 73 – *Physical Security Certification and Accreditation*; and

c. the need for secure communications Capability between Project stakeholders (for further information regarding the requirement for secure communications, refer to DSPF Principle 10 - *Classification and Protection of Official Information*.)

43. For small Project teams, the Integrated Project Manager may fulfil the role of Security Officer for a Project (refer to *DSPF Governance and Executive Guidance* (4a) regarding Security Officer roles and responsibilities.)

Defence Special Access Programs Project Managers

44. Project Managers responsible for Defence Projects that include Special Access Program (SAP) activities are to maintain the special security requirements applicable to the SAP framework. DI(G) ADMIN 62-1 Defence Special Access Programs—*Policy and Management* (classified CONFIDENTIAL) assigns responsibilities and prescribes security procedures for implementation and use in the management, administration and oversight of all Defence SAPs.

Key Definitions

45. **Project**. A unique, finite, multidisciplinary and organised endeavour to realise agreed FIC deliverables within pre-defined requirements and constraints.

46. **Project Manager**. The person who has responsibility to plan and deliver the Project, inclusive of all agreed FIC to the specified scope, schedule and budget.

Note: *Reference to Integrated Project Managers refers to Project managers engaged in Projects conducted as part of the Capability Life Cycle (CLC) process.*

47. **Integrated Project Management Team**. The organisational entity established within the primary delivery and enabler Group which performs Project functions as part of the Capability Life Cycle process. It is comprised of representatives from all relevant stakeholders.

48. **Project Sponsor**. The primary representative of the Capability Manager and the Program Sponsor liaising directly with the Integrated Project Manager. The Project Sponsor is accountable to the Capability Manager and Program Sponsor for delivery of the Product. The Project Sponsor sets direction for the Project and ensures that activities and outputs are consistent with the Capability needs and priorities of the Capability user.

49. **Program Manager**. The person appointed within the delivery and enabler Group to conduct program management functions in support of acquisition and sustainment activities.

50. **Program Sponsor**. The person accountable for ensuring that the outcomes of all program activities are achieved and that these outcomes remain aligned with Defence strategic objectives. The Program Sponsor is accountable to the Capability Manager for the management of Capability throughout the Capability Life Cycle.

51. **Resident project teams**. Defence personnel, Contractors, Consultants or Outsourced Service Providers based overseas with foreign prime contractors on Defence acquisition Projects.

52. **Capability**. The power to achieve a desired operational effect in a nominated environment, within a specified time, and to sustain that effect for a designated period. Capability is generated by FIC comprising organisation, personnel, collective training, major systems, supplies, facilities, support, command and management, and industry.

53. **Project Identification Document (PID)**. A document that provides information about the Project or Project phase. A PID indicates the anticipated level of protectively marked information and/or assets to be protected, in-country and overseas industry involvement, and likely ICT connectivity requirements.

54. **Security Classification and Categorisation Guide (SCCG)**[1]. A document that records the security classification and Business Impact Level (BIL) given to each element of a Project or asset.

55. **Program/Project Security Instruction (PSI)**. A document that outlines how whole of Government and Defence program/Project security measures will be applied to the Project.

56. **Special Access Program (SAP)**. A high security, Capability protection framework that imposes need-to-know and access controls beyond those normally provided for access to PROTECTED, CONFIDENTIAL, SECRET, or TOP SECRET information. The level of controls is based on the criticality of the program to the Defence mission and the assessed hostile intelligence threat. The program may be an acquisition program, an intelligence program, or an operations and support program.

Further Definitions

57. Further definitions for common PSPF terms can be found in the Glossary.

58. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

[1] SCCGs were previously known as Security Classification Grading Documents (SCGD).

Document administration

Identification

DSPF Control	Security for Projects
Control Owner	Assistant Secretary Program Management (AS PM)
DSPF Number	Control 11.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Security for Projects
Related DSPF Control(s)	Security for Capability Planning

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 PM	Launch

Defence Security Principles Framework (DSPF)

Security for Capability Planning

General Principle

1. The security of capabilities acquired, and their ongoing management, is to be considered at all stages of the Capability Life Cycle.

Rationale

2. Failure to consider and forecast security requirements during capability development and throughout the Capability Life Cycle, including assessing the security impacts on all Fundamental Inputs to Capability (FIC), could lead to operational failure, project delays and increased costs.

Expected Outcomes

3. Capabilities are delivered uncompromised in terms of security and are maintained as such throughout their lifecycle.

4. Domain Leads, Program Sponsors, Project Managers and System Program Offices (SPO) apply security controls throughout and project activities and budget for them accordingly.

5. Security guidelines are contained in the Capability Life Cycle.

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 Investment Portfolio (ASIP)
High	Defence Security Committee (DSC) – through ASIP
Extreme	DSC – through ASIP

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Security for Capability Planning
Principle Owner	First Assistant Secretary Security and Vetting Service
DSPF Number	Principle 12
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	N/A
Control Owner	Assistant Secretary Investment Portfolio

Related information

Government Compliance	**PSPF Core Requirements:** Security Planning; Security governance for contracted service providers; and Eligibility and suitability of personnel.
Read in conjunction with	Interim Capability Life Cycle Manual
See also DSPF Principle(s)	Classification and Protection of Official Information Security for Projects Physical Security Access Control Procurement
Implementation Notes, Resources and Tools	• Australian Government physical security management protocol • ASIO, Security Equipment Guides (SEGs) are available from the GovDex Protective Security Community

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 Jule 2018	FAS S&VS	Launch

Defence Security Principles Framework (DSPF)

Communications Security (COMSEC)

General principle

1. Defence protects the confidentiality, integrity and availability of its electronic communications. This is achieved through measures and controls necessary to deny unauthorised persons access to electronic communications, and ensuring the authenticity of such communications.

Rationale

2. Communications security (COMSEC) is essential to protect the confidentiality and integrity of electronic communications. Most Defence information is processed and communicated via electronic means. Protecting this information from adversaries and inadvertent disclosure is essential for Defence to carry out its mission successfully.

Expected outcomes

3. Defence personnel, contractors, consultants and outsourced service providers with access to COMSEC information and material are aware of their responsibilities.

4. Access to COMSEC information and material is limited to Defence personnel, Contractors, Consultants and Outsourced Service Providers who have:

a. a demonstrated need-to-know;

b. a security level of clearance commensurate with the information and material being accessed; and

c. been appropriately briefed. See the underlying DSPF Control and the Australian Communications Security Instructions (ACSI) suite.

5. Defence personnel, Contractors, Consultants and Outsourced Service Providers are debriefed on their continued responsibilities once the requirement for access to COMSEC material ceases for any reason.

Escalation Thresholds

6. The Information Technology Security Advisor (ITSA) has set the following general threshold for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence ITSM	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Advisor. **Note**: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Appointed Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Communications Security (COMSEC)
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 13
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 13.1
Control Owner	Information Technology Security Adviser (ITSA)

Related information

Government Compliance	**PSPF Core Requirements:** Reporting on Security; and Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology system. Australian Government Information Security Manual (ISM) Australian Communications Security Instructions (ACSIs) **Legislation:** *Workplace Health and Safety Act 2011* *Crimes Act 1914* *Defence Act 1903* *Criminal Code Act 1995*
Read in conjunction with	N/A
See also DSPF Principle(s)	Security for Projects Security for Capability Planning Information Systems Security Incident Management Defence Industry Security Program Overseas Travel Access Control Identification, Search and Seizure Regime Security Incidents and Investigations

Implementation Notes, Resources and Tools	• ACSI suite of documents • ADFP 6.0.3.1 Communications Security Instructions • ADFP 6.0.3 Information Assurance • Policy Broadcast 02/2010: Transportation • DI(G) CIS 6-2-002 – High Assurance Cryptographic Equipment Provision • 2017 ISM, Cryptographic Fundamentals • Australian Government, Physical Security Management Guidelines—Security Zones and Risk Mitigation Control Measures.

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	CISO	Launch

Defence Security Principles Framework (DSPF)

Communications Security (COMSEC)

Control Owner

1. The Information Technology Security Advisor (ITSA) is the Control Owner for this control under the Administration & Governance Domain of the administrative policy framework (which includes security).

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Communications Security (COMSEC)
Control Owner	Information Technology Security Adviser (ITSA)
DSPF Number	Control 13.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Communications Security (COMSEC)
Related DSPF Control(s)	Security for Projects Security for Capability Planning Information Systems Security Incident Management Defence Industry Security Program Overseas Travel Access Control Identification, Search and Seizure Regime 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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Audio-visual Security

General principle

1. Classified information is to be protected from deliberate and accidental compromise through technical means.

Rationale

2. The communication of classified information is vital for Defence's objectives; however this information can be of great value to unauthorised persons who may undertake technical surveillance to acquire it. It is important for Defence Staff to be aware of these threats and to take appropriate measures to ensure classified communications and the integrity of classified spaces are protected from audio-visual surveillance.

Expected outcomes

3. Defence protects the confidentiality and integrity of its communications from technical surveillance or compromise by adopting necessary measures and controls to maintain the integrity of classified spaces and deny access to unauthorised persons.

4. Defence can communicate classified information in a manner that does not compromise its operations.

Escalation Thresholds

5. The Assistant Secretary Security Threats and Assurance (ASSTA) 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 Security Officer, Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Director Security Intelligence and Threats – through Defence Security and Vetting Service Technical Surveillance Countermeasures Team.
High	ASSTA
Extreme	Defence Security Committee – through ASSTA

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Audio-visual Security
Principle Owner	First Assistant Secretary Security and Vetting Service
DSPF Number	Principle 14
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 14.1
Control Owner	ASSTA

Related information

Government Compliance	**PSPF Core Requirements**: Classification of information; Access to information; Safeguarding information from cyber threats; Robust information and communication technology systems; and Entity resources. ASIO Technical Notes 5/12 & 1/15 Australian Signals Directorate's Information Security Manual (ISM) **Legislation**: *Crimes Act 1914*, *section 70* and *79* *Defence Act 1903*, *section 73A* *Criminal Code Act 1995*, *Division 91* **Standards**: ISO/IEC 27035:2011 International standard for information security incident management (Due to become ISO/IEC 27035) Australian Communications Security Instruction (ACSI) Suite
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Information Systems (Physical, Personnel and Logical) Security Personnel Security Clearance Temporary Access to Classified Information and Assets Overseas Travel Working Offsite Physical Transfer of Information and Assets

Implementation Notes, Resources and Tools	• ACSI-101(B) – Communication Security (General), section 6: outlines the Australian Signals Directorate's (ASDs) whole-of-government responsibilities as the Australian National COMSEC Authority; • ACSI-53(E) - Communications Security Handbook (Rules and Procedures for the Agency COMSEC Officer and Custodian); • ADFP 6.0.3.1 Communications Security Instructions, noting in particular access requirements in paragraphs 53.44 and 53.46; • DI(G) CIS 6-2-002 – High Assurance Cryptographic Equipment Provision; • Australian Signals Directorate's Information Security Manual (ISM), 2016 ISM Controls, Cryptographic Fundamentals, Controls, pg 236; • Australian Government Information security management guidelines—Australian Government security classification system – provides guidance to assist agencies in identifying the value of information, resulting in the application of a suitable protective marking; • Australian Government, Physical security management guidelines—Security zones and risk mitigation control measures; • Australian Government Information security management guidelines – Protectively marking and handling sensitive and security classified information - provides guidance on procedures for applying protective markings and information handling procedures; and • Australian Government Information Security Manual - sets out the standard governing the security of Australian Government ICT systems.

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

Defence Security Principles Framework (DSPF)

Audio-visual Security

Control Owner

1. The Assistant Secretary Security Threat and Assurance (ASSTA) is the owner of this enterprise-wide control.

2. Assistant Director Technical Surveillance and Countermeasures (TSCM) provides TSCM certification services and audio-visual security advice, through the Director Security Intelligence and Threats, for ASSTA.

3. Defence Security and Vetting Service (DS&VS) is the TSCM authority within Defence.

4. ASSTA is responsible for:

a. the provision of advice regarding audio-visual security compliance requirements and technical standards;

b. providing advice and services to designate a facility as audio-secure as a part of the accreditation process; and

c. ascertaining that the facility is physically suitable for use as an audio-secure room at the level required (refer Annex A of this Control - *Construction and Acoustic Testing of Audio Secured Rooms*).

Escalation Thresholds

5. ASSTA 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 Security Officer, Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Director Security Intelligence and Threats through the DS&VS TSCM
High	ASSTA
Extreme	Defence Security Committee – through ASSTA

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Audio-visual Security

6. Audio-visual security is measures undertaken to secure classified information from compromise by unauthorised persons through surveillance or other technical collection methods. Ensuring that classified information is communicated within appropriately security accredited facilities is the primary measure taken to mitigate audio-visual security risks. Modern, well-concealed, covert surveillance devices (bugs) are unlikely to be detected in the short term, prior to harm being caused. The first line of defence is appropriate protective security.

Key Definitions

7. Audio-security level (ASL) is a designation that describes the level of audio-security certification of a facility. A Certified Audio Secure Room is a room that is rated ASL3 or above and has been certified as audio secure.

8. TSCM is the term to describe methods taken to identify and mitigate potential technical vulnerabilities or a deliberate audio or visual attack. TSCM measures are implemented to reduce the vulnerability of technical compromise of classified discussions.

9. Such countermeasures also apply to covert video interception of proceedings. TSCM certification within Defence is carried out as a part of the security accreditation process and is conducted by appropriately trained TSCM technicians. Training is provided by DS&VS and other Australian government agencies. See ‘Arranging a TSCM inspection’ below for further information.

Audio Secure Facilities

10. Access to rooms with audio security measures should be strictly controlled. Access should be limited to authorised persons with the appropriate security

clearance, briefings and need to know. Refer to the DSPF Principle72 - *Physical Security* and the DSPF Principle 74 - *Access Control for more information*.

11. Table 1 describes the appropriate audio secure facilities for classified conversations. Audio secure facilities are rated (ASL) in accordance with a measure of audio privacy.

Table 1 – Audio Secure Facilities Appropriate for Classified Conversations

Facility use	Requirement
Regular UNCLASSIFIED / PROTECTED discussions, or Ad-Hoc (irregular – no more than once each month) SECRET discussions	ASL 2
Regular SECRET, or Ad-Hoc TOP SECRET	ASL 3
SECRET (Amplified Speech)	ASL 3 +
TOP SECRET	ASL 4 or above
TOP SECRET, amplified Sensitive Compartmented Information (SCI)	ASL 5

+ denotes a requirement of an acoustic weighted level difference (Dw) rating increase of 5 points due to speech amplification IAW ASIO Technical Note 1/15

12. Control Implementers and Control Officers are to consider the relevant risks and obtain advice from the DS&VS TSCM unit or the compartment controllerASL 2 rated rooms may be used at a higher ASL rating after seeking advice from the DS&VS TSCM unit, and will require a risk assessment that is available to the Control Owner.

13. Facilities rated lower than ASL 3 are not normally subject to TSCM testing unless special circumstances are identified through liaison between the Control Implementer and DS&VS TSCM.

14. If classified meetings or activities are required in a Defence facility that is not normally maintained for audio-security, advice on security requirements is to be obtained from the DS&VS TSCM. Meetings or activities held at SECRET and above in non-accredited facilities are not to be held without prior approval by the Control Owner (ASSTA), or Australian Signals Directorate Defence Intelligence Security (ASD DIS) if at TOP SECRET. In seeking this approval, Control Implementers should undertake a security risk assessment, considering the mitigations listed in ASIO Technical Note 1/15 para 16.8.

15. If an audio-secure room with a suitable ASL rating is not available, Control Implementers may allow irregular meetings up to the SECRET level in a room if the risks involved are adequately assessed and managed in accordance with the Risk Escalation Thresholds for this Control. Advice from DS&VS TSCM is available to

inform this risk assessment. In these circumstances Control Implementers are also to:

a. ensure that anyone in adjoining areas is cleared and authorised for access to the material to be discussed;

b. put in place measures to ensure that nobody is allowed to loiter in adjoining corridors;

c. document the frequency and nature of such arrangements, which may be subsequently used as evidence for creation and certification of an audio-secure room; and

d. ensure signage is placed on all entry doors and on or near any equipment that is used to generate amplified speech. These signs will indicate that local Standard Operating Procedures (SOPs) apply when using this equipment for classified conversions.

Authority to Vary the Audio Standards for Audio-Secure Rooms

16. The Control Owner may approve the variation of the audio secure standards for rooms up to and including the SECRET level following a risk assessment from the Control Implementer.

17. Only the relevant compartment controller may vary requirements for TOP SECRET compartmented material. Any audio-secure room that comes under internationally agreed audio-security requirements is not to be modified without the permission of the compartment controller.

Electronic Equipment within Certified Audio-Secure Rooms

18. Any electronic device that can store or transmit information that is brought into an audio secure room can compromise classified discussions. Devices that are not appropriately classified and/or accredited are not to be taken into audio secure rooms. For information on selecting appropriate ICT equipment and electronic devices, refer to:

a. DSPF Principle 22 - *Mobility Device Security*;

b. DSPF Principle 72 - *Physical Security*;

c. DSPF Principle 73 – *Physical Security Certification and Accreditation*;

d. DSPF Principle 23 - *ICT Certification and Accreditation*; and

e. Information Security Manual (ISM) Controls.

19. Electronic equipment in audio-secure rooms need to be approved as a part of the certification and accreditation process, and advice should be sought on adding any equipment to an existing room.

20. The following describes the electronic requirements that cannot be used:

a. The area is not to have installed any unaccredited audio or video transmitters, wireless microphones, intercom systems, facsimile equipment, public address systems or cordless telephones; and

b. Other devices capable of transmitting or recording sound or video (including mobile phones) are not to be brought into the room unless their purpose is to overtly record a meeting. If this is the case, the device(s) are to be declared to the Security Officer, and the device(s) and media are to be classified, registered and labelled according to the maximum classification of the material recorded; refer to DSPF Principle 22 – *Mobility Device Security* for further information.

Exclusion: *Accredited Defence laptops identified and classified as SECRET or higher may be brought into the room on a temporary basis if they are classified at or above the current activity within the room.*

Classified Conversations in Non-Audio Secure Spaces

21. **Off-site** - classified conversations are to be protected from being overheard when conducted off-site, refer DSPF Principle 70 – *Working Offsite* for further information.

22. **Open plan facilities** - open plan offices present an increased security risk as conversations can be overheard by those that are not appropriately cleared or do not have a need to know. Personnel in open plan spaces are:

a. to consider moving their discussion to an accredited audio secure space;

b. to ensure that all personnel within hearing range hold an appropriate security clearance and have a genuine need-to-know before discussing classified material. Personnel should also ensure no Portable Electronic Devices (PEDs) or other items that may present a risk to the discussion are in the vicinity; and

c. not to discuss TOP SECRET material unless the entire open plan facility is a designated Zone Five (refer DSPF Principle 72 - *Physical Security* for descriptions of Physical Security Zones).

Amplified Speech

23. Audio amplification is any electronically distributed content such as video conference, teleconference and speaker phone, amplified for the purpose of sound

distribution. Where amplified classified speech is generated the audio is to remain within the physical boundaries of that certified audio-secure room.

24. A risk assessment should be completed prior to installing equipment generating amplified speech in certified audio secure rooms.

25. These systems are not to be installed in any Zone Five unless they have been accredited by the area's Physical and ICT Accreditation Authorities.

Hearing Augmentation in Conferencing Facilities

26. The National Construction Code requires facilities (such as conference rooms, video conference, theatres) in certain circumstances to be fitted with a hearing augmentation system. DS&VS TSCM can provide advice on acceptable listening systems for hearing augmentation where required.

27. The listening system is to be designed so as it can be physically isolated from the main audio-visual system until it is required. The transmission signal of the hearing augmentation system is to be contained within the audio-secure facility.

Operational Deployments, Trials and Exercises

28. Long-term operational deployments are to be treated in the same manner as a fixed secure-facility in Australia, if possible. If deemed not possible, a security risk assessment should be undertaken in accordance with the Risk Escalation Threshold of this Control. Control Implementers should seek the advice from the DS&VS TSCM when setting up audio-secure facilities while on operations.

29. In the case of short-term operational deployments, trials and exercises, Control Implementers can determine the need for audio-security, particularly where other measures have been taken to ensure security of the facility or area. Control Implementers should undertake a security risk assessment, taking into consideration the history and location of a fixed facility and the possibility of audio-security compromise. Advice on mitigating these risks can be sought from DS&VS TSCM and records should be made available to the Control Owner. These requirements only apply to SECRET and below spaces. For TOP SECRET spaces refer to ASD DIS.

ADF Platforms

30. TSCM inspections and testing on Australian Defence Force platforms are conducted on a needs basis with consultation from DS&VS and ASD DIS. As a Control Implementer, if the Unit Commander has a concern with or requires advice on audio-security, the DS&VS TSCM can be contacted directly or through the Service Security Adviser.

Arranging a TSCM Inspection

31. TSCM tests are conducted to determine whether unauthorised devices have been placed in an accredited audio secure facility. TSCM tests are not a guarantee of

long-term audio integrity, which can only be assured by the appropriate use of protective security measures and access controls.

32. TSCM tests are to be conducted periodically in audio-secure facilities, and before conferences and meetings in other facilities, if deemed necessary after a security risk assessment and consultation with DS&VS TSCM.

33. The Control Implementer responsible for the security of a certified audio-secured room is to arrange TSCM services:

a. for periods not exceeding five years, or in accordance with advice from DS&VS TSCM;

b. following any actual or suspected compromise of an audio-secure room;

c. following any works, alterations, furniture and appliance changes or other activity which may have introduced a security risk to an audio-secure room; or

d. when the Control Owner considers that TSCM testing is warranted.

34. To request TSCM services please contact via the Defence Secret Network - DSVSTSCM@dsn.mil.au. Knowledge of a forthcoming TSCM inspection should be restricted to staff with a need to know. A TSCM inspection can provide a high level of assurance about an area's technical security and assists in lessening the risks, but it does not guarantee that the area is free from the risk of technical compromise. If an intended TSCM inspection is well known, covert surveillance devices may be removed.

Actions on Finding a Suspected Intelligence Collection Device

35. The discovery of a suspected intelligence collection device is a major security incident and the following actions are to be completed:

a. cease all classified discussions;

b. do not touch, move, or test the object; and

c. immediately:

   i. report it to the relevant Control Implementer and/or Unit Security Officer;

   ii. secure the facility, if practical, so the suspect device cannot be removed; and

   iii. report the discovery to the DS&VS Security Incident Centre (SIC) as a MAJOR Security Incident. (refer DSPF Principle 77 - *Security Incidents and Investigations*, and consider the classification of the

incident report. Guidance on submitting a Security Incident Report at SECRET and above can be found here).

Further Definitions

36. Further definitions for common PSPF terms can be found in the Glossary.

37. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – *Constructing Audio-Secure Rooms*.

Document Administration

Identification

DSPF Control	Audio-visual Security
Control Owner	ASSTA
DSPF Number	Control 14.1
Version	2
Publication date	27 September 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Audio-visual Security
Related DSPF Control(s)	Classification and Protection of Official Information Information Systems (Physical, Personnel and Logical) Security Personnel Security Clearance Temporary Access to Classified Information and Assets Overseas Travel Working Offsite Physical Transfer of Information and Assets

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	ASSTA	Launch
2	27 September 2018	ASSTA	Removed the ASL requirement for UNCLASSIFIED discussions in Table 1

Annex A to Audio-visual Security – Construction and Acoustic Testing of Audio Secured Rooms

Construction of Audio Secured Rooms

1. Audio-secured rooms are constructed to:

a. minimise or prevent unauthorised access;

b. provide evidence of any attempted or actual physical penetration or audio attack;

c. minimise the number of places where devices could be located; and

d. facilitate audio Technical Surveillance Countermeasures (TSCM) testing.

2. The services of an accredited acoustics engineer are to be sought for design advice and build consultation. On completion of the works, the acoustics engineer provides a formal weighted level difference (Dw) certification.

3. A TSCM certification **must** be conducted at the end of construction as a contribution to the audio-security rating of the room, consult the Defence Security and Vetting Service (DS&VS) for further advice.

Additional Considerations

4. The construction standards shown below are designed for a room in isolation, however, the following considerations may apply:

a. if a room is located within a secure area that is rated at an equal or higher level, some of the construction and acoustic requirements may be reduced depending on the surrounding environment;

b. if the risk of accidental compromise, such as overhearing, is high, the audio attenuation may need to be increased to a level above the minimum standard for that room; and

c. for areas located within heritage listed buildings, careful consideration and alternatives will be required to maintain audio and physical security while complying with the construction standard constraints.

5. Advice is to be obtained from the Group or Service Security Authority and DS&VS TSCM on a case-by-case basis.

Audio-Secure Level 4 Rooms

6. Table 1 outlines the minimum requirements for the construction of an audio-secure level (ASL) 4 room. This is to be read in conjunction with the Australian Security and Intelligence Organisation (ASIO) Tech Notes ATN1-15 & ATN5-12 Physical Security of Zones & Physical Security of Zone 5 (Top Secret) Areas.

Table 1 – Minimum Requirements for the Construction of an ASL 4 Room

Component	Requirements
Room location	The room shall be an internal room with corridors on all outside walls so there are no adjoining rooms. Corridors are to have controlled access, particularly when the room is in use. It is best practice to: a. locate the room on the upper or basement level to minimise access above and below the room; and b. control access to rooms and corridors above and below the protected area.
Dw rating	The acoustic attenuation weighted level difference (Dw) rating of the room shall be: c. Dw 45, including above any false ceiling and around doors and windows; and d. tested on-site by Certified Acoustic Testing Engineers to AS/NZS 717.1:2004 standards.
Construction materials	Construction and lining materials for all six sides shall be selected from suitable material to meet the Dw rating.
Walls and ceilings	Walls are to be of slab-to-slab construction. Walls and ceilings shall be of tamper evident construction. Do not use relocatable partitioning or wallpaper. DS&VS recommends a surface finish of a light coloured, gloss paint.

Component	Requirements
Doors	Doors are to be: a. constructed with a block board core; b. fitted with Security Construction Equipment Committee (SCEC)-approved mortice locks; and c. able to be secured from the inside. To achieve the Dw rating, doors may require: a. fitting with acoustic drops; b. soundproof lining on the doorjamb; and c. covers on internal keyholes. The use of an airlock is recommended where possible and where double doors are required it is usually the most practical way to achieve the Dw rating.
Windows	DS&VS recommends that windows or glass panels are not used in audio-secure rooms. If windows are used: a. external windows are to be double glazed; b. fit scrim curtains to prevent over viewing; and c. keep windows locked.
Other features	DS&VS recommends a security alarm system for times when the room is unoccupied; If public address speakers are required for emergency evacuation: a. fit each speaker with isolation amplifiers; or b. replace speakers with lights and buzzers in piezo alarms. Treat air-conditioning or service ducts with acoustic baffles and lining.

Audio-Secure Level 3 Rooms

7. Table 2 outlines the minimum requirements for the construction of an ASL 3 room. This is to be read in conjunction with ASIO Tech Note ATN1-15 Physical Security of Zones.

Table 2 – Minimum Requirements for the Construction of an ASL 3 Room

Component	Requirements
Room location	If the Dw rating is achieved, speech privacy rooms may share common walls with other rooms. DS&VS recommends that speech privacy rooms do not adjoin public areas or waiting rooms.
Noise Isolation Class (NIC) rating	The acoustic attenuation Dw rating of the room shall be: a. Dw 40, including above any false ceiling and around doors and windows; and b. tested on site by Certified Acoustic Testing Engineers to AS/NZS 717.1:2004 standards. If a public address system will be used, the Dw rating may require upgrading.
Construction materials	Construction and lining materials for all six sides shall be selected from material to meet the NIC rating.
Doors	Doors are to be: a. constructed with a block board core; b. fitted with SCEC-approved mortice locks; and c. able to be secured from the inside. To achieve the Dw rating doors may require: a. fitting with acoustic drops; b. soundproof lining on the doorjamb; and c. covers on internal keyholes.

Component	Requirements
Walls and ceilings	DS&VS recommends that walls be of slab-to-slab construction. If this is not possible, either: a. prevent access by: (1) a fixing 3 mm thick, 12 mm x 19 mm opening size Expanded Metal Mesh in the false ceiling between the top of the perimeter wall partitioning and the ceiling slab; (2) welding the mesh to 38 mm x 38mm steel angle fixed to the underside of the ceiling slab with Loxins or similar and screw-fixed to the top of the wall partitioning; and (3) welding the mesh panels to each other to form a single unit; or b. maintain controlled access to the ceiling space with alarms and locks on access panels. Outside walls are to be kept free of plant growth for at least 500 mm to allow the walls to be inspected. If wall partitioning finishes at a drop or false ceiling, install a 50 mm sound attenuation blanket extending 600 mm on each side of the partition.
Other components	Treat air-conditioning or service ducts with acoustic baffles and lining. Lock windows.

Acoustic Testing of Audio Secure Rooms

8. Acoustic testing is carried out by an appropriately qualified Audio Engineer on a room or area to establish audio attenuation and to identify any points of weakness. The testing is also conducted to determine whether a facility has met the required benchmarks for the level classified discussions that will take place within the confines of the area

9. Rooms intended for sensitive activity usage are tested to specific audio standards to minimise:

a. the risk of accidental audio compromise where intelligible speech can be heard from the room by someone in an adjacent space or transiting past; and

b. the risk of a deliberate technical attack utilising audio leakage where covert access into the controlled space is not easily possible.

Requirements

10. The average sound pressure level should be achieved by the following:

a. the use of the enlarged frequency range as per AS/NZS 717.1:2004;

b. using a single microphone moved from position to position, or by an array of fixed microphones, as per AS/NZS 717.1:2004 and IS0 140-4 and not by a continuously moving or oscillating microphone;

c. the position of the microphone locations should be such that they cover the weakest points in the area/room (such as doors, windows, and penetrations). The purpose of this test is to ascertain whether any sound is flanking around a building element rather than through the building element material;

d. the test report should contain the average results and point/position measurement data including the results of any weak points identified;

e. the test report should also include a diagram of the test area indicating test points used and weak point identified; and

f. the average result is to meet the appropriate audio level for the designated audio-secured room type.

11. Point/position measurements should meet the appropriate audio level for the designated audio-secured room type. If a point/position measurement failure occurs the result may or may not require rectification depending on a risk assessment undertaken by DS&VS TSCM, as the certifying authority. DS&VS TSCM will consider variation approaches provided that, in its opinion, the overall outcome remains within acceptable risk tolerance.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Construction and Acoustic Testing of Audio Secured Rooms
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Audio-visual Security
DSPF Number	Control 14.1

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	ASSTA	Launch

Defence Security Principles Framework (DSPF)

Foreign Release of Official Information

General principle

1. The release of information to foreign services, organisations, or nationals must balance the benefits of sharing information against the likelihood and consequences of security harm.

Rationale

2. The release of official information to foreign governments, foreign organisations and foreign nationals is a key operational requirement for the pursuit of Defence objectives.

Expected outcomes

3. Appropriate consideration of the risk/benefit for the release of official information.

4. Sharing of information in accordance with agreed safeguards and controls.

5. Formal risk assessments are undertaken for foreign release requests outside of the scope of Defence-specific Security of Information Agreements and Arrangements (SIA)/ Whole-of-Government Security of Information Agreements and Arrangements (GSA).

Escalation Thresholds

6. Foreign Release of UNCLASSIFIED information with a Dissemination Limiting Marker (DLM)

Risk Rating	Responsibility
Low	EL1/O5 or equivalent in relevant Group/Service
Moderate	EL2/O6 or equivalent in relevant Group/Service
Significant	EL2/O6 or equivalent in relevant Group/Service
High	EL2/O6 or equivalent in relevant Group/Service
Extreme	EL2/O6 or equivalent in relevant Group/Service

7. Foreign Release of CLASSIFIED information under a GSA/SIA

Risk Rating	Responsibility
Low	EL2/O6 or equivalent in relevant Group/Service
Moderate	EL2/O6 or equivalent in relevant Group/Service
Significant	Assistant Secretary Security Policy and Services (AS SPS)
High	AS SPS
Extreme	First Assistant Secretary Security & Vetting Service (FAS S&VS)

8. Foreign Release of CLASSIFIED information outside of a GSA/SIA

Risk Rating	Responsibility
Low	Director Industry & International Security Policy (DS&VS)
Moderate	AS SPS
Significant	AS SPS
High	FAS S&VS
Extreme	FAS S&VS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Foreign Release of Official Information
Principle Owner	First Assistant Secretary Security & Vetting Service (FAS S&VS)
DSPF Number	Principle 15
Version	2
Publication date	23 November 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 15.1
Control Owner	Assistant Secretary Security Policy and Services

Related information

Government Compliance	**PSPF Core Requirements**: Security governance for contracted service providers; Security governance for international sharing; Eligibility and suitability of personnel; Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems. ISM Control Principles
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information
Implementation Notes, Resources and Tools	Australian Government, Information security management guidelines, protectively marking and handling sensitive and security classified information

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	23 November 2018	FAS S&VS	Correct Escalation Table, paragraph 6; correct Control Owner position title; add additional related information.

Defence Security Principles Framework (DSPF)

Foreign Release of Official Information

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this Control.

Escalation Thresholds

2. Foreign Release of UNCLASSIFIED information with a Dissemination Limiting Marker (DLM)

Risk Rating	Responsibility
Low	EL1/O5 or equivalent in relevant Group/Service
Moderate	EL1/O5 or equivalent in relevant Group/Service
Significant	EL2/O6 or equivalent in relevant Group/Service
High	EL2/O6 or equivalent in relevant Group/Service
Extreme	EL2/O6 or equivalent in relevant Group/Service

3. Foreign Release of CLASSIFIED information under a Whole-of-Government Agreement (GSA)/Defence-specific Agreement (SIA)

Risk Rating	Responsibility
Low	EL2/O6 or equivalent in relevant Group/Service
Moderate	EL2/O6 or equivalent in relevant Group/Service
Significant	AS SPS
High	AS SPS
Extreme	First Assistant Secretary Security & Vetting Service (FAS S&VS)

4. Foreign Release of CLASSIFIED information outside a Whole-of-Government Agreement (GSA)/Defence-specific Agreement (SIA)

Risk Rating	Responsibility
Low	AS SPS
Moderate	AS SPS
Significant	AS SPS
High	FAS S&VS
Extreme	FAS S&VS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Control

Why does Defence need a Foreign Release Request Process?

5. The release of official information to foreign governments, foreign organisations and foreign nationals may advance Defence's organisational objectives.

What is the Foreign Release process for UNCLASSIFIED information?

6. UNCLASSIFIED information without a DLM can be released to all parties on a need to know basis.

7. UNCLASSIFIED information with a DLM can be released to all parties on a need to know basis if written approval is given by the originator.

The following text should be provided with any UNCLASSIFIED DLM information released: *This information is official Australian Government information. Unauthorised disclosure is not permitted and the information is not to be released to third parties or third countries without written approval from the originator. Any suspected or actual loss or compromise of the information is to be reported immediately to the originator.*

What is a Release Authority?

8. A Release Authority is an official at a specified rank/level who can make an informed determination about whether to approve or deny a foreign release request. Foreign release outside of a GSA/SIA is also subject to approval from AS SPS.

What is an Information Sharing Agreement/Arrangement?

9. The Australian Government can enter into an Agreement or Arrangement with another country that specifies the conditions under which official information can

be exchanged. These also establish security classification equivalencies. They can be SIAs or GSAs. When an SIA/GSA is in place it makes the process of exchanging classified information easier, as both parties have agreed to safeguard each other's classified information in a manner consistent with their own practices.

10. GSA/SIAs with intergovernmental organisations do not cover foreign releases to member governments or to the private nationals of member states i.e. the Australia-NATO SIA cannot cover a foreign release request to Bulgaria. This would require an explicit Australia-Bulgaria SIA/GSA.

What is the Foreign Release Process Under an SIA/GSA?

11. To release classified information under an SIA/GSA you should obtain the formal approval of a Release Authority at the EL-2/O6 level or higher. To get this approval you should provide them with the following:

a. A statement outlining the scope of the release approval e.g. an individual document/information related to a specific project or activity;

b. A statement outlining the purpose of the release e.g. is it information to support a training activity? Is it information related to a classified contract?

c. Details about the end recipient, e.g. is the information being released to an individual? is the information being released to a government/organisation?;

d. Written advice from the originator of the information supporting its release;

Note: *If Defence-originated information is not subject to a caveat, it is to be treated as approved by the originator for release to FVEY governments (FVEY refers to an alliance comprising Australia, Canada, New Zealand, the United Kingdom and the United States).*

e. If releasing to a foreign industry partner, formal verification of the recipient's facility security clearance to the standard required under the GSA/SIA; and

f. If releasing to an individual recipient, formal verification of the recipient's personnel security clearance to the standard required under the GSA/SIA.

12. The officer acting as the Release Authority should consider whether the information provided in the request is sufficient to justify a release and inform the requester of their decision.

What SIA/GSAs are Currently in Effect?

13. A list of UNCLASSIFIED GSAs/SIAs is available on the Defence Protected Network.

14. If you are unsure whether a GSA/SIA exists, or if it would cover your specific circumstances, please contact Industry and International Security Policy (IISP) within Defence Security and Vetting Service.

When Would a GSA/SIA Not Apply?

15. GSA/SIAs only apply when releasing classified information to individuals where the individual is either directly connected to their government i.e. as a contractor/public servant/member of the armed forces, or they hold a personnel security clearance provided by that government. If an individual foreign national has no security clearance and is unable to gain one from their home government, then a foreign release request will need to be undertaken outside of a GSA/SIA.

What is the Foreign Release Process for Classified Information Outside of an SIA/GSA?

16. To request the foreign release of classified information not covered by a SIA/GSA you should first obtain the formal approval of a Release Authority at the SES-1/07 level or higher. To get this approval you should provide them with the following:

a. A statement outlining the scope of the release approval (e.g. is the approval for an individual document? All classified information up to a certain classification related to a specific operation/activity? All classified information relating to a specific project?);

b. A statement outlining the purpose of the release (e.g. is it information to support a training activity? Is it information relating to a classified contract?);

c. Details about the end recipient (is the information being released to an individual? Is it being released to a government/organisation?);

d. Written advice from the originator of the information supporting its release;

e. A formal risk assessment covering the release (see below); and

f. An outline of any proposed mitigation measures.

17. The officer acting as the Release Authority should consider whether the information provided in the request is sufficient to justify a release and inform the requester of their decision.

18. The requester **must** then send the release request, along with written advice from the Release Authority, to AS SPS for approval. AS SPS will review the request, make a final decision about whether the release is approved, and inform the Release Authority of their decision.

Note: *The Release Authority should aim to provide material supporting the foreign release to AS SPS at least 3 weeks prior to the release date.*

What is Required in a Formal Risk Assessment?

19. A formal risk assessment should assess the likelihood and consequence of the information being used in a manner contrary to Australia's interests. For example, what is the potential for the information to be:

a. used inappropriately;

b. unintentionally released to a third party; or

c. intentionally released to a third party.

20. If one of these things were to happen, what would the nature of the impact be to:

a. Australia's national security?

b. Defence capability?; and/or

c. International relations?

21. You should seek advice to assist in the completion of your risk assessment from DIISP.

Is Information Marked with the AUSTEO Caveat Subject to the Foreign Release Request Process?

22. Classified information marked with the AUSTEO caveat cannot be released to foreign governments, foreign organisations or foreign nationals.

Is Information Marked with the AGAO Caveat Subject to the Foreign Release Request Process?

23. Yes, but only in very limited circumstances (Five Eyes nationals integrated in, or working on behalf of the Australian Government, and meeting all of the additional requirements outlined in DSPF Principle 10 - *Classification and Protection of Official Information*. In all other circumstances, classified information marked with the AGAO caveat cannot be released to foreign governments, foreign organisations or foreign nationals.

Is Information Marked with the RELEASABLE TO (REL) Caveat Subject to the Foreign Release Request Process?

24. The REL caveat identifies information that can be released to the indicated countries without following the foreign release request process. Foreign release requests to countries not listed in the marking are subject to the normal foreign release request process.

Further Definitions

25. Further definitions for common PSPF terms can be found in the Glossary.

26. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Foreign Release of Official Information
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)
DSPF Number	Control 15.1
Version	2
Publication date	23 November 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Foreign Release of Official Information
Related DSPF Control(s)	Classification and Protection of Official Information

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 SPS	Launch
2	23 November 2018	AS SPS	Refine foreign release process for Unclassified DLM/Sensitive level information.

Defence Security Principles Framework (DSPF)

Defence Industry Security Program

General Principle

1. The Defence Industry Security Program (DISP) provides confidence and assurance in the secure delivery of goods and services to the Department of Defence (Defence) when partnering with industry.

Rationale

2. DISP is a risk management program that strengthens security practices in partnership with industry, and enables members to have their security practices recognised by Defence and Defence's international industrial security partners.

3. DISP enhances Defence's ability to manage risk in the evolving security environment and provides confidence and assurance to Defence and other government entities (either Australian or foreign) when procuring goods and services from industry members.

4. DISP sets minimum security standards required for industry to partner on projects at the Unclassified/DLM, PROTECTED, SECRET and TOP SECRET levels.

5. DISP membership forms part of Defence's security risk mitigations and does not remove the requirement for contracting areas to undertake a project security risk assessment. Contracting areas are responsible for managing the security risks of their projects when partnering with industry. For further information, see DSPF Principles 11, 12, and 82.

Expected Outcomes

6. Accountabilities and responsibilities for security risk management when procuring goods and services are understood and practised.

7. Security risks are effectively and efficiently managed between Defence and industry.

8. DISP:

a. supports Defence's agility in achieving value for money in procurement;

b. provides effective and efficient mechanisms for certifying and accrediting industry's security practices;

c. enables increased access to security tools and information to strengthen industry security practices; and

d. delivers confidence and assurance when partnering with industry, underpinned by proportional (risk based) oversight and compliance activities.

Escalation Thresholds

Risk Rating	Responsibility
Low	Assistant Director Industry & International Security Policy
Moderate	Director Industry & International Security Policy
Significant	Assistant Secretary Security Policy and Services
High	First Assistant Secretary Security and Vetting Services
Extreme	Defence Security Committee – through Assistant Secretary Security Policy and Services

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Defence Industry Security Program
Principle Owner	First Assistant Secretary Security and Vetting Service
DSPF Number	Principle 16
Version	2
Publication date	9 April 2019
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 16.1
Control Owner	Assistant Secretary Security Policy and Services

Related information

Government Compliance	**PSPF Core Requirements**: Security governance for contracted service providers. **Legislation**: *Privacy Act 1988* (Cth) **Standards**: AS: 4811-2006: Employment screening
Read in conjunction with	N/A
See also DSPF Principle(s)	Personnel Security Clearance Temporary Access Classification and Protection of Official Information Information Systems (Physical, Personnel and Logical) Security Foreign Release of Official Information Physical Transfer of Official Information, Security Protected and Classified Assets
Implementation Notes, Resources and Tools	DS&VS Defence Industry Security Program webpage AGSVA FAQ Page

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	9 April 2019	FAS S&VS	DISP Reform Launch

Defence Security Principles Framework (DSPF)

Defence Industry Security Program

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner for this control.

Escalation Thresholds

Risk Rating	Responsibility
Low	Assistant Director Industry & International Security Policy
Moderate	Director Industry & International Security Policy
Significant	Assistant Secretary Security Policy and Services
High	First Assistant Secretary Security and Vetting Services
Extreme	Defence Security Committee – through Assistant Secretary Security Policy and Services

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

The Program

2. Industry Entities (Entities) **must** hold an appropriate level of Defence Industry Security Program (DISP) membership when working on classified information or assets; storing or transporting Defence weapons or explosive ordnance; providing security services for Defence bases and facilities; or as a result of a Defence business requirement specified in a contract.

3. The exception to this is where an Entity:

a. has accreditation recognised under a Security of Information Agreement or Arrangement (SIA); or

b. personnel are handling classified information within Defence facilities and using Defence assets (ICT networks).

4. DISP membership is also encouraged for those wishing to supply goods and services to Defence and other government entities (either Australian or foreign).

5. DISP membership provides industry with the information, services, and support they need to manage security risks and protect sensitive information and assets in line with Defence security requirements. These services include personnel security vetting, certification and accreditation of facilities and/or ICT systems.

6. DISP membership supports industry partnerships and supply chain security.

7. Entities can self-nominate to join DISP independent of having a contract with Defence.

Membership

8. To attain and maintain DISP membership, Entities **must** meet the DISP eligibility and suitability requirements.

9. DISP membership is not automatic; Defence will assess the eligibility and suitability of each application in consultation with relevant Australian Government agencies, such as the Australian Security Intelligence Organisation.

10. The DISP Privacy Notice covering the collection, use, storage, disclosure and disposal of applicant's information is at Annex A of this Control.

11. While there is no membership fee, Entities are responsible for covering the indirect costs associated with applying for, and maintaining DISP membership. Indirect costs include but are not limited to:

a. personnel security clearances (vetting fees and charges are available on AGSVA's website);

b. time and travel to attend training (such as the Security Officer course); and

c. implementing all governance, personnel, physical, and information & cyber security requirements relevant to their chosen level of membership.

12. The First Assistant Secretary Security and Vetting Services (FAS S&VS) is responsible for granting DISP membership. FAS S&VS may delegate this authority to the Director Industry and International Security Policy (EL2), or an appropriate EL1 appointed within this section.

Eligibility

13. To be eligible for DISP membership an Entity **must**:

a. be registered as a legal business entity in Australia;

b. be financially solvent;

c. have a designated officer who can obtain an Australian security clearance in order to fulfil the role of a Chief Security Officer (CSO). The Chief Security Officer **must** be a member of the entity's board of directors (or similar governing body), executive personnel, general partner, or senior management official with the ability to implement policy and direct resources. They **must** be able to obtain and maintain a Baseline security clearance;

d. have a designated officer who can fulfil the role of Security Officer (SO). A Security Officer **must** be able to obtain and maintain a Baseline security clearance (for Entry Level membership) or the minimum of a NV1 security clearance (for membership Levels 1, 2 and 3). This position may have the ability to nominate and sponsor clearances within the business, as outlined in this policy. If necessary, the Chief Security Officer, and Security Officer, may be the same individual;

e. have a contact email address to facilitate correspondence, in the form of disp@insertbusinessname.xxx.xx (different domain names are accepted);

f. satisfy Defence that the Entity does not have any Foreign, Ownership, Control or Influence (FOCI) affecting the management or operations of the Entity, in a manner which could result in unauthorised access to classified information or adversely affect the performance of contracts.

   (1) FOCI is defined as when a foreign interest has the power, direct or indirect, whether or not exercised, and whether or not exercisable, through the ownership of the company under the purview of its National Security Authority/Designated Security Authority, by contractual arrangements or other means, to direct or decide matters affecting the management or operations of that entity in a manner which may result in unauthorised access to classified information or adversely affect the performance of classified contracts or may otherwise be contrary to the interests of national security.

g. not have any relationships with a listed terrorist organisation. For more information see https://www.nationalsecurity.gov.au/listedterroristorganisations/pages/default.aspx;

h. not have any relationships with regimes subject to Australian sanctions laws including the United Nations Security Council (UNSC) sanctions regimes and Australian autonomous sanctions regimes. For more information see http://dfat.gov.au/international-relations/security/sanctions/sanctions-regimes/Pages/sanctions-regimes.aspx; and

i. not have any relationship with persons and/or entities on DFAT's Consolidated List. The Consolidated List includes all persons and entities to which the *Charter of the United Nations Act 1945* and the *Autonomous Sanctions Act 2011* currently applies. This follows the transition of Australia's targeted financial sanctions from the *Banking (Foreign Exchange) Regulations 1959* to the *Autonomous Sanctions Regulations 2011. For more information see* http://dfat.gov.au/international-relations/security/sanctions/Pages/consolidated-list.aspx.

14. Defence, through the FAS S&VS may deny, downgrade, suspend or terminate DISP membership if it is determined that granting or continuing a membership is not in Defence's or the national interest, or if the eligibility and suitability criteria are not met.

Suitability

15. An Entity that meets the eligibility requirements can apply for DISP membership by submitting a DISP application and FOCI form.

16. Once submitted, Defence will conduct an assessment to confirm eligibility and determine suitability.

17. Additional information and/or documentation may be required from the applicant to enable Defence to make this assessment.

18. The DISP Suitability Matrix at Annex B of this Control specifies the minimum membership requirements for each level and element of the DISP. Applicants self-nominate the membership level that best meets their entity's requirements.

19. To be granted DISP membership, all applicants **must** meet the minimum requirements for Entry Level governance, personnel security, physical security and information/cyber security.

20. Applicants can apply for a higher level(s) of membership for individual elements of the DISP where they meet the minimum requirements. For example, a DISP member can apply for personnel security at level 2, and information and physical security at entry level, if this best suits their needs or contract requirements. While personnel, physical and information/cyber security elements can be accredited individually at different membership levels, the governance security element **must** be equivalent to the highest level of accreditation sought for the other elements of membership.

Ongoing Suitability

21. DISP members **must**:

a. safeguard Defence and industry's people, information and assets;

b. comply with the DSPF, including where applicable; its referenced authoritative documents such as the Information Security Manual (ISM) and relevant Defence policies covering physical, personnel and communication security policies and practices. Where the DSPF does not specify a policy position, industry should refer to the PSPF for guidance;

c. appoint and retain a CSO, and trained SO (the CSO and SO can be the same individual);

d. report any changes that may affect their DISP membership in accordance with the relevant requirements of the DSPF, including but not limited to:

(1) eligibility and suitability changes;

(2) FOCI changes;

(3) security and fraud incidents (See DSPF Principle 77 – Security Incidents and Investigations);

(4) contact with foreign officials; and

(5) changes in circumstances for their security cleared personnel (e.g. contact details, relationship status, financial changes, overseas travel. See DSPF Control 40.1 – Personnel Security Clearances);

e. comply with all audit and assurance activities at the direction of the Defence Security and Vetting Service (DS&VS), including completion of the Annual Security Report (ASR) every 12 months from the date of DISP membership;

f. keep a register of overseas travel and travel briefings, and make it available to Defence upon request.

Security Incident & Foreign Contact Reporting

22. A security incident is an occurrence which results, or may result, in negative consequences for the security of Defence, or a breach of controls in the PSPF, DSPF or the Information Security Manual.

23. A security incident **must** be reported by the DISP member in accordance with Defence Policy (see DSPF Principle 77 – Security Incidents and Investigations).

24. DISP members **must** keep a register of all security incidents, and make it available to Defence upon request.

25. DISP Members **must** report all foreign contact (suspicious, ongoing, unusual and/or persistent contact with a foreign national(s)), in accordance with Defence Policy (see DSPF Principle 45 – Contact Reporting).

Upgrading or Downgrading Membership

26. A DISP member may apply to upgrade or downgrade their membership level for specific elements of the DISP, as appropriate for their business requirements, or in order to meet contractual requirements.

Contract Managers

27. Contract Managers **must** notify DS&VS where DISP membership is a contract requirement. Contract managers **must** provide DS&VS with the following information:

a. the Defence representative contact details;

b. the Entity Defence is engaging with;

c. details of the contract/panel/partnership;

d. the security requirements of the contract/partnership including DISP membership levels. For example governance level ‘x’, personnel security level ‘x’, physical security level ‘x’, information/cyber security level ‘x’.

Assurance

28. The DISP assurance framework consists of five core elements:

a. Compliance with DISP eligibility and suitability requirements (certification and accreditation);

b. Annual Security Report (ASR);

c. Intelligence led assurance program;

d. Five year forward audit work program, and

e. Shipbuilding assurance program.

29. To ensure compliance with the DISP minimum security requirements, Defence will:

a. undertake assurance and compliance activities;

b. review DISP member’s ASR annually;

c. conduct random and targeted security checks of DISP members, this may include but is not limited to, a review of the company’s security policies and plans, personnel, information and physical security arrangements and security registers, including physical security inspections;

d. assess industry security incident, fraud and contact reports, in accordance with DSPF; and

e. conduct security investigations as appropriate, in accordance with DSPF.

30. DISP assurance activities will also inform the CASG Company Performance ScoreCard rating.

a. The CASG ScoreCard assesses a company's past performance while under contract, using defined criteria and provides a performance rating for each category. Further information on the ScoreCard process can be found here.

International Recognition

31. The Australian Government (including Defence) manages Security of Information Agreements and Arrangements (SIA) in place with many countries for the protection and exchange of classified information. Some of these Agreements and Arrangements also provide for the recognition of personnel and facility clearances.

32. These allow for:

a. DISP members to engage in contracts generating or providing access to classified information with foreign governments and companies under those governments' jurisdiction; and

b. foreign companies to participate in contracts for the Australian Government or Entities, generating or providing access to classified information even though they may not be DISP members.

33. To confirm the existence of an International SIA, where possible, please visit the Current Agreements and Arrangements page or the Australian Treaties Database, otherwise enquires should be directed to dsvsdsp.international@defence.gov.au.

34. To confirm the existence of personnel security clearances of foreign entities, enquires should be directed to securityclearances@defence.gov.au.

35. To confirm the existence of facility security clearances of foreign entities, enquires should be sent to facility.securityclearances@defence.gov.au.

Australian Community

36. On 5 September 2007 the Australian and the United States (US) Governments signed the Treaty between the Government of Australia and the Government of the United States of America concerning Defense Trade Cooperation (the Treaty). The Treaty is intended to improve the efficiency of eligible two-way transfers between Australia and the US by facilitating the export of controlled goods without the need for an export licence. This was achieved through the creation of an

Approved Community in Australia and the US which includes government and private facilities. Approved agencies in Australia are referred to as the Australian Community (AC).

37. The AC is managed by Defence Export Controls and is separate to the DISP. Defence Export Controls can be contacted at ExportControls@defence.gov.au.

Prioritisation Framework

38. Defence will process DISP applications in line with the following priority order:

a. P1 – Your company is in a contract with Defence in direct support of a Defence Operation;

b. P2 – Your company is in a contract with Defence;

c. P3 – Your company is actively planning to tender, or in negotiations for a Defence opportunity; or

d. P4 – Your company is applying for DISP with no existing relationship to Defence and no immediate tender opportunities.

Roles and Responsibilities

Defence

39. Defence is responsible for:

a. acting in good faith;

b. providing information and support for joining the DISP;

c. processing membership applications in a timely manner;

d. providing ongoing security management advice;

e. providing the timely provisioning of services to certify and accredit facilities and ICT networks (see DSPF Principle 23 – ICT Certification and Accreditation, and Principle 73 – Physical Security Certification and Accreditation);

f. providing vetting services through AGSVA; and

g. upholding all responsibilities as per the policy framework.

Industry Entities

40. Industry Entities are responsible for:

a. acting in good faith;

b. ensuring information provided is not deceptive or misleading;

c. applying the “need to know principle”;

d. ensuring no unauthorised access (including by third parties) to official/classified information or materials;

e. providing all relevant information required to assess their eligibility and suitability for DISP membership; and

f. where applicable, meeting all security requirements specified by Defence, and any Australian government entities or foreign government entities in contract and/or a SIA.

Chief Security Officer

41. The CSO **must** be an Australian citizen and be able to obtain and maintain a Personnel Security Clearance at the Baseline level or above, as appropriate with the Entity’s level of DISP membership.

42. The CSO is responsible for oversight of, and responsibility for, security arrangements and championing a security culture in the Entity. They have the flexibility to delegate the day-today management of protective security to SO(s), where required.

43. The CSO is accountable for ensuring:

a. all obligations contained in the DISP principle and control policy documents for their level of membership are met;

b. an appropriate system of risk, oversight and management is maintained;

c. DISP reporting obligations are fulfilled;

d. sensitive and classified materials entrusted to the Entity are safeguarded at all times;

e. Security Officer(s) are appointed to develop and implement the Entity’s security policies and plans, on the CSO’s behalf;

f. DISP Annual Security Report is agreed by the executive (Board equivalent), and all recommendations are implemented within agreed timeframes; and

g. any change in Foreign Ownership Control and Influence (FOCI) status of the Entity is reported to Defence via the FOCI Declaration (AE250-1).

44. If the CSO for an Entity changes, the Entity is to notify Defence by emailing DISP.submit@defence.gov.au. The Entity is to provide the information located in Part 5A of the Application Form (AE250).

Security Officer

45. The SO **must** be an Australian citizen and be able to obtain and maintain a Personnel Security Clearance at the Baseline level or above, as appropriate with the Entity's level of DISP membership.

46. The SO is responsible for:

a. the development and application of security policies and plans within each establishment;

b. ensuring sensitive and classified materials entrusted to the Entity are safeguarded at all times;

c. maintaining the Designated Security Assessed Position (DSAP) list (Level 1 and above), which is to be made available to DS&VS at their request;

d. the management of personnel security clearance requests;

e. reporting change of circumstances and vulnerabilities of clearance holders;

f. facilitating annual security awareness training of personnel;

g. reporting security incidents and fraud incidents, and contact reports, in accordance with Defence policy; and

h. yearly assurance activities to support the CSO.

47. SO's may not sponsor personnel security clearances requiring an eligibility waiver. Where the exceptional circumstances criteria are met within the Australian Government's Protective Security Policy Framework, SO's are to consult with the control owner regarding clearance sponsorship for individuals requiring an eligibility waiver(s).

48. If an SO for an Entity changes, the Entity is to notify Defence by emailing DISP.submit@defence.gov.au. The Entity is to provide the information located in Parts 5B and 5C of the Application Form (AE250).

Ceasing Industry Security Program Membership

49. DISP membership will continue until such time as it is voluntarily ceased by the DISP Entity; or downgraded, suspended or terminated by Defence.

Voluntary withdrawal or ceasing

50. Industry Entities can voluntarily withdraw from the application process at any stage, or cease their membership by notifying Defence via email to DISP.submit@defence.gov.au.

51. Upon withdrawal or ceasing, Defence will notify all Defence Project/Contract Manager(s) and non-Defence entities that requires DISP membership as a condition of contract.

Terminating, suspending or downgrading membership

52. Non-compliance with DISP membership requirements may result in Defence downgrading, suspending or terminating an Entity's DISP membership.

53. With the exception of downgrading, suspension or termination there are no other penalties associated with the failure to comply with DISP membership requirements under the DISP. Failure to comply with DISP membership requirements may have other consequences, for example:

a. contractual penalties where obligations to meet a contractual requirement are not met; or

b. criminal or financial penalties or sanctions under Australian law.

54. A suspension is a time-limited operating constraint suspending that Entity's ability to operate as a DISP member. It may also prevent the Entity from bidding for further work with Defence, and/or restrict its ability to sponsor security clearances until the security issues that led to the suspension are rectified.

55. Downgrading or suspension can be imposed upon the whole Entity, an accredited facility or an ICT system. Personnel security clearances associated with the Entity may become inactive if DISP membership is suspended. If the DISP membership is terminated, the clearances sponsored by Defence, and clearances sponsored by the Entity under the DISP membership, will become inactive. Where there are multiple interested parties in a clearance subject, those parties will be given the opportunity to assume sponsorship so that the clearance remains active.

56. AS SPS will consult with affected parties prior to a decision to downgrade, suspend or terminate an Entity's DISP membership.

57. The decision to downgrade, suspend or terminate an Entity's DISP membership is to be made by FAS S&VS and cannot be delegated.

Obligations and Consequences

58. When DISP membership ceases:

a. where applicable, any sensitive or classified information or materials belonging to a project or program **must** be returned or destroyed in accordance with the contract terms and conditions;

b. the CSO and nominated SO's security clearances that were obtained for the purposes of DISP membership will cease to be sponsored by DS&VS and become inactive;

c. all DISP member's personnel security clearances will also become inactive unless sponsorship is assumed by a multiple interested party;

d. facility and ICT system accreditation will lapse; and

e. Defence will notify affected parties (those that are related to a contracted project or program) of ceased memberships.

Dispute Resolution, Procedural Fairness, Appeals and Reviews

Dispute resolution

59. Dispute resolution should occur at a level that is proportionate and commensurate with the risk posed to Defence and the achievement of the project outcome.

60. Complaints should be made in the first instance to the Director Industry and International Security Policy, DS&VS.

61. If resolution at that level is unsuccessful, complaints should be escalated to the AS SPS, and then to FAS S&VS.

Procedural Fairness

62. Where a DISP membership is being considered for denial, downgrade, suspension or termination, the Entity is entitled to procedural fairness before the decision is made about the membership. DS&VS will inform the Entity of the reasons for the recommendation, to the fullest extent allowable within national security provisions, and afford the Entity the opportunity to respond.

63. Where a membership is denied or revoked, the principles of procedural fairness require that any subsequent administrative actions are not undertaken until any appeals by an Entity are finalised.

64. At any time, if a significant security concern is identified, notwithstanding procedural fairness provisions, FAS S&VS retains the right to temporarily suspend or

remove an Entity's access to security services, including suspension or termination of Physical or ICT certification, accreditation and/or withdrawing sponsorship of personnel security clearances and the ability to sponsor clearances.

Appeals and Reviews

65. Where DS&VS denies, downgrades, suspends or terminates a DISP membership, the Entity may appeal the decision. DS&VS will inform the Entity of the relevant avenue(s) of appeal when notifying them of an adverse membership decision.

Key Definitions

66. **Industry Entity (Entity)**: An entity (such as a sole trader, partnership, trust, company or university) that is registered as an Australian business and is located within the territory of Australia.

67. **Contract Manager:** For the purposes of this policy, Contract Managers are defined as Defence personnel responsible for managing Defence contracts; this could include but is not limited to, Program Managers, Project Managers, Senior Project Officers, Project Officers or any other role with contract manager responsibilities.

Annexes

Annex A – Defence Industry Security Program – Privacy Notice

Annex B – Defence Industry Security Program – Suitability Matrix

Document Administration

Identification

DSPF Control	Defence Industry Security Program
Control Owner	Assistant Secretary Security Policy and Services
DSPF Number	16.1
Version	2
Publication date	9 April 2019
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Defence Industry Security Program
Related DSPF Control(s)	Personnel Security Clearance Temporary Access Classification and Protection of Official Information Information Systems Security (Physical, Personnel and Logical) Foreign Release of Official Information Physical Transfer of Information and Assets Security Incidents and Investigations Procurement

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 SPS	Launch
2	9 April 2019	AS SPS	DISP Reform Launch
3	10 April 2019	AS SPS	Update

Defence Security Principles Framework (DSPF)

Annex A to Defence Industry Security Program – Privacy Notice

Defence Industry Security Industry Program Privacy Notice

1. Defence Industry Security Program (DISP) resides within the Department of Defence (Defence) and is a risk mitigation and assurance program maintaining the integrity of Australia's Defence capability. DISP sets out to safeguard the supply chain by ensuring defence industry maintains its security responsibilities. DISP enhances Defence's ability to monitor and mitigate the security risks associated with the contracting for, or outsourcing of, services, functions and capabilities. Defence Security and Vetting Services (DS&VS) on behalf of Defence will undertake a risk based assessment in order to confirm your eligibility for DISP membership. In order to meet the membership requirements Defence will ask you to provide information about your company, including your level of foreign ownership, control and influence (FOCI). This privacy notice outlines how Defence collects, uses, and discloses personal information.

How your information will be collected and to whom it may be disclosed

2. The DISP process undertakes a risk based assessment on your Entity's suitability to gain and maintain DISP membership. In order to process your DISP application and make a determination, Defence may share your personal information with other relevant Australian Government agencies including but not limited to:

- Australian Security Intelligence Organisation (ASIO) and/or Australian Signals Directorate (ASD) to facilitate the membership assessment.

3. With your consent, Defence may share your personal information to support tenders for work or contracts with:

- Other Government agencies; or
- International Partners under an SIA.

The purpose for collecting your information

4. Personal information is collected to assess your entities eligibility to hold and maintain DISP membership. It is important to note that failure to provide accurate information required for this assessment may result in a failure to obtain DISP membership and will impede on your ability to apply for DISP membership in the future. Your company information may also be used in the identification, management and investigation of security threats and incidents and to undertake investigations into suspected breaches of law or of Australian Government policy.

Accessing and updating your information

5. For information about how Defence holds your personal information, how you can apply for access to, or seek a correction of personal information Defence holds about you, or to make a complaint about how Defence has managed your personal information, you should refer to the Defence Privacy Policy.

6. Questions regarding the Defence Privacy Policy, or privacy within Defence, should be emailed to the Defence Privacy Office defence.privacy@defence.gov.au or sent via regular mail to:

Defence Privacy Office
BP35-1-065
PO Box 7927
CANBERRA BC ACT 2610

Additional Resources

7. The *Privacy Act 1998*

Further information can be found at Defence Privacy Policy.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document administration

Identification

DSPF Annex	Defence Industry Security Program – Privacy Notice
Annex Version	1
Annex Publication date	9 April 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Industry Security Program
DSPF Number	Control 16.1

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	9 April 2019	AS SPS	DISP Reform Launch

Defence Security Principles Framework (DSPF)

Annex B to Defence Industry Security Program – Suitability Matrix

	Governance*	Personnel Security	Physical Security	Information and Cyber Security
Entry Level	• Maintain an appropriate system of risk oversight and management (i.e. risk register including security considerations). • Provide business details • Provide points of contact • Must have a nominated Chief Security Officer (CSO) (must be able to meet AGSVA eligibility requirements for Baseline clearance) • Must have a nominated Security Officer (SO) (must be able to meet AGSVA eligibility requirements for Baseline clearance) • SO may request access to the DISP Security Portal, to access security documents, templates, forms and tools which include: o assurance reporting forms, security policy and plans templates, risk assessment forms etc., • Security Officer Training Course is optional for nominated SO and CSO however the SO is to complete the Introduction to DISP course • Annual Security Awareness Course must be completed by all personnel • Security Officer must understand and effectively manage personnel/facilities and information and cyber security up to an Unclassified/DLM level • Maintain and implement Security Policies and Plans • Insider threat program • Business security risk assessment • Reporting and management of security incidents and foreign contacts • Report changes in Foreign Ownership Control & Influence • Conduct travel briefings • Complete annual assurance activities • Annual Security Report	• SO has no ability to sponsor security clearances • Provide a description of employment screening practices • AS 4811—2006 Employment screening is the minimum standard for all new recruitments	• Provide a description of physical security and access controls at each facility and their location	• Must meet one of the following standards across all of the Entity's ICT corporate networks used to correspond with Defence: - The following four requirements of the ASD Essential 8: o application whitelisting; o patch applications; o restrict administrative privileges; and o patch operating systems - Unclassified/DLM network in accordance with the ISM/DSPF - ISO/IEC 27001/2:2013 *Information security management* - NIST SP 800-171 Rev.1 *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations* (US ITAR requirement) - Cyber security for defence suppliers (Def Stan 05-138) • Provide a description of information and cyber security practices and accreditations.

	Governance*	Personnel Security	Physical Security	Information and Cyber Security
Level 1	**All governance requirements from the Entry Level, plus:** • Complete annual assurance activities • Security Officer required to maintain a NV1 clearance • Security Officer understands and effectively manages personnel/facilities and Information and cyber security up to and including PROTECTED level • Security Officer Training Course is required for the SO, but optional for the CSO. • SO may request access to the Security Officer Dashboard for the ability to sponsor security clearances • Maintain a list of Designated Security Assessed Positions (DSAP)	**All personnel requirements from the Entry Level, plus:** • Security Officer has the ability to sponsor Baseline security clearances • Ensure Baseline cleared personnel adhere to ongoing security clearance requirements	**All physical requirements from the Entry Level, plus:** • Ensure facilities are certified and accredited in accordance with the DSPF to receive, handle, store and destroy PROTECTED information and material	**All information & cyber requirements from the Entry Level, plus:** • Ensure a PROTECTED network or standalone device is employed in accordance with the ISM/DSPF
Level 2	**All governance requirements from Level 1, plus:** • Security Officer must understand and effectively manage personnel/facilities and Information and cyber security up to and including SECRET level	**All personnel requirements from the Entry Level, plus:** • Security Officer has the ability to sponsor security clearances up to NV1 • Ensure Baseline and NV1 cleared personnel adhere to ongoing security clearance requirements • Ensure compartment holders adhere to compartment requirements	**All physical requirements from the Entry Level, plus:** • Ensure facilities certified and accredited in accordance with the DSPF to receive, handle, store and destroy SECRET information and material	**All information & cyber requirements from the Entry Level, plus:** • Ensure a SECRET network or standalone device is employed in accordance with the ISM/DSPF
Level 3**	**All governance requirements from Level 2, plus:** • If applicable, Security Officer trained in compartment briefings obligations – COMSO course • Security Officer must understand and effectively manage personnel/facilities, and Information and cyber security up to and including TOP SECRET level***	**All personnel requirements from the Entry Level, plus:** • Security Officer has the ability to sponsor security clearances up to NV2 • Ensure Baseline, NV1 and NV2/PV cleared personnel adhere to ongoing security clearance requirements • Ensure compartment holders adhere to compartment requirements	**All physical requirements from the Entry Level, plus:** • Ensure facilities certified and accredited in accordance with the DSPF to receive, handle, store and destroy TOP SECRET information and material	**All information & cyber requirements from the Entry Level, plus:** • Ensure a TOP SECRET network or standalone device is employed in accordance with the ISM/DSPF

* Governance security must always match or exceed the highest level of membership sought for any other category.

** SES Band 3 sponsorship is required to obtain a Positive Vetting clearance / certification and accreditation of Secure Compartment Information Facility (SCIF) and TOP SECRET network.

*** Note: the management of compartment briefs will be managed by a Defence Communications Intelligence Security Officer (COMSO).

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Defence Industry Security Program – Suitability Matrix
Annex Version	1
Annex Publication date	9 April 2019
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Industry Security Program
DSPF Number	Control 16.1

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	9 April 2019	AS SPS	DISP Reform Launch

Defence Security Principles Framework (DSPF)

Information Systems (Physical) Security

General principle

1. Defence will protect ICT systems and networks with physical security controls that are proportionate to the assessed risks, which are informed by the confidentiality, integrity and availability business impacts applicable to the ICT asset.

Rationale

2. Defence personnel with a need to know and an appropriate level of clearance are able to securely access information from, and communicate with, information systems and electronic communications devices as required.

3. The security of Defence and Defence Industry Information Communications and Technology (ICT) systems is dependent on the physical context in which they operate. The degree of physical access could significantly affect the security risks to a system or network, regardless of geographic location.

Expected outcomes

4. Defence protects Information Communication and Technology (ICT) systems and networks with physical security controls that are proportionate to the assessed risks, which are informed by confidentiality, integrity and availability business impacts applicable to the asset;

5. Physical security controls are integrated with procedural, logical and personnel security controls, which are applied to ICT systems and networks in accordance with the Australian Signals Directorate's (ASD) *Information Security Manual (ISM)*; and

6. High Assurance Products and Controlled Cryptographic Items are physically secured in accordance with DSPF Principle 13 – *Communications Security (COMSEC)*, and applicable *Australian Communications Security Instructions (ACSIs)*.

Escalation Thresholds

Risk Rating	Responsibility	
	CIOG managed or connected systems	**Group/Service managed systems**
Low	EL1/05 within the Directorate of Regional ICT Services (DRICTS), ICT Security Branch Integrated Risk Management (IRM) Directorate or Information Technology Security Manager (ITSM)	EL1/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	EL2/O6 within DRICTS, ICT Security Branch IRM Directorate or ITSM	EL2/O6 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor (CSA) **Note**: In the event that an appointment of a Group or Service CSA has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive (DSE) **Note**: In the event that an appointment of a Group or Service CSE has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Defence Chief Information Officer (CIO)	Appointed Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Information Systems (Physical) Security
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 17
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 17.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	**PSPF Core Requirements**: Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems. Australian Government Information Security Manual **Standards:** • AS/NZS 2053 - Conduits and fittings for electrical installations • AS/CA S009:2013 Installation requirements for customer cabling (Wiring Rules) • AS 3996-2006 Access covers and grates, where appropriate • AS/NZS 3084:2017 Telecommunications installations – Telecommunications pathways and spaces for commercial buildings
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Security for Projects Communications Security (COMSEC) Offshore and Cloud Based Computing ICT Certification and Accreditation Information Systems Security Incident Management Information Systems Business Impact Levels and Aggregation Access Control Security Incidents and Investigations

Implementation Notes, Resources and Tools	• Australian Government information security management guidelines – Australian Government security classification system – provides guidance to assist agencies to identify the value of information, and, in turn, apply a suitable protective marking; • Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and material – provides guidance on procedures for applying protective markings and information handling procedures; • Australian Government Information Security Manual – sets the out the standard governing the security of Australian Government ICT systems.

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	CISO	Launch

Defence security principles framework (DSPF)

Information Systems (Physical) Security

Control Owner

1. Information Technology Security Advisor (ITSA) is the Control Owner for this policy.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Information Systems (Physical) Security
Control Owner	Information Technology Security Advisor (ITSA)
DSPF Number	Control 17.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems (Physical) Security
Related DSPF Control(s)	Classification and Protection of Official Information Security for Projects Communications Security (COMSEC) Offshore and Cloud Based Computing Security ICT Certification and Accreditation Information Systems Security Incident Management Information Systems Business Impact Levels and Aggregation Access Control 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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Information Systems (Personnel) Security

General principle

1. Defence will ensure that Information Communications and Technology (ICT) systems are only accessed by authorised users who hold a Defence personnel security clearance at, or above, the required level, and who have a demonstrated need-to-know.

Rationale

2. Confidence in the security of an ICT system can only be maintained if personnel security is applied to the systems users.

3. Different users present different security risks to Defence and Defence Industry information systems. For this reason, Defence needs to understand the mix of users of it systems and ensure that the right information is available to the right people at the right times.

Expected outcomes

4. Defence ICT systems are only accessible by authorised personnel with:

a. an appropriate level of clearance; and

b. a demonstrated need-to-know.

5. The number of privileged users is kept to a minimum and regularly reviewed.

6. Privileged users are only assigned the minimum amount of privileges to be able to perform their assigned tasks related to their role and responsibilities.

7. Foreign nationals are only able to access information that is releasable to their nationality. On the rare occasions when privileged access by foreign nationals is required, it is tightly controlled.

Escalation Thresholds

8. The Information Technology Security Advisor (ITSA) has set the following general threshold for risks managed against this Defence Security Principles

Framework (DSPF) Enterprise-wide Control and the related DSPF Principle and Expected Outcome.

Residual Risk Rating	**Responsibility**	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Group or Service Cyber Security Executive **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Group or Service Cyber Security Executive **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (CIO) (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Information Systems (Personnel) Security
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 18
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 18.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	**PSPF Core Requirements**: classification of Information; access to Information; safeguarding information from cyber threats; and robust information and communication and technology systems. *Australian Government Information Security Manual (ISM)*
Read in conjunction with	N/A
See also DSPF Principle(s)	Information Systems (Logical) Security Mobility Device Security Identity Security Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Government information security management guidelines – *Australian Government security classification system* Australian Government information security management guidelines – *Protectively marking and handling sensitive and security classified information and material* *Australian Government Information Security Manual (ISM)*

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	CISO	Launch

Defence Security Principles Framework (DSPF)

Information Systems (Personnel) Security

Control Owner

1. The Information Technology Security Advisor (ITSA) is the Owner for this Enterprise-wide Control.

2. The Accountable Officer for the Information and Communications Technology domain is the Chief Information Officer. The ITSA also works under this domain.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

3. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

4. Further definitions for common PSPF terms can be found in the Glossary.

5. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Information Systems (Personnel) Security
Control Owner	Information Technology Security Advisor (ITSA)
DSPF number	Control 18.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems (Personnel) Security
Related DSPF Control(s)	Information Systems (Logical) Security Mobility Device Security Protcted Identities Access Control 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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Information Systems (Logical) Security

General principle

1. Defence will protect ICT systems and networks with logical security controls that are proportionate to the assessed risks, which are informed by confidentiality, integrity and availability business impacts applicable to the ICT asset.

Rationale

2. Information security (logical) systems and associated procedures provide assurance and protection to the confidentiality, integrity, and availability of systems and the information within them.

Expected outcomes

3. Defence personnel is to ensure appropriate permissions are received before providing third parties access to Defence ICT Systems and networks not originating from Defence. Defence and Defence Industry ensure that appropriate security measures have been taken to protect official, sensitive, and classified Defence information from unauthorised use, access, or accidental modification, loss or release;

4. Defence and Defence Industry only use Defence ICT systems and networks in a manner that is appropriate and in accordance with DSPF Principle 10 - *Protection of Official Information and Assets*; and

5. Defence personnel is to ensure appropriate permissions are received before providing third parties access to Defence ICT Systems and networks not originating from Defence.

Escalation Thresholds

6. The Information Technology Security Advisor (ITSA) has set the following general thresholds for risks managed against this *Defence Security Principles Framework (DSPF) Enterprise-wide Control* and the related *DSPF Principle and Expected Outcomes.*

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	Information Communications Technology (ICT) Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Advisor Note: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (CIO) (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Appointed Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Information Systems (Logical) Security
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 19
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 19.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	**PSPF Core Requirements**: Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems **Legislation**: *Electronic Transactions Act 1999* *Telecommunications (Interception and Access) Act 1979* *Archives Act 1983* **Standards**: *Australian Government Information Security Manual (ISM)* *Australian Defence Force Communications Instruction (ADFCI) 6.2.5 Radiocommunications Monitoring Procedures*
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Security for Projects Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems Log Management Offshore and Cloud Based Computing Remote Access to Defence Systems
Implementation Notes, Resources and Tools	Australian Government Information Security Manual – sets out the standard governing the security of Australian Government ICT systems

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	CISO	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems (Logical) Security

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments

Document administration

Identification

DSPF Control	Information Systems (Logical) Security
Control Owner	Information Technology Security Advisor (ITSA)
DSPF number	Control 19.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principles and Expected Outcomes	Principle 19 Information Systems (Logical) Security
Related DSPF Control(s)	N/A

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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Information Systems Lifecycle Management

General principle

1. The security of Defence information systems will be managed throughout all stages of the system's lifecycle.

Rationale

2. Defence depends on its Information and Communications Technology (ICT) to deliver vital services in support of military operations and Defence business. Risks to Defence ICT systems can arise at a number of points throughout the lifecycle of a system, from design or acquisition, through development or operational usage, to decommissioning and disposal. The most effective use of security resources is achieved by considering security risks from the earliest stages of the system lifecycle.

Expected outcomes

3. All internally developed and commercially obtained systems address security requirements as part of their systems lifecycle.

4. Security is considered from the earliest stages of system development.

5. Systems are designed, built, managed and decommissioned in accordance with the Australian Government Information Security Manual (ISM) and relevant ISO standards.

6. Defence appoints a System Sponsor and System Owner for all production systems and they maintain an awareness of the system, security boundaries, and residual security risks for the systems which they are responsible for.

7. Defence, specifically the system owners across the members of the Groups and Services, who have responsibility for the ICT systems throughout the system lifecycle, understand its information assets and maintain an inventory of the systems on which they reside.

Escalation Thresholds

Residual Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence ITSM	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor. **Note**: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point.
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Information Systems Lifecycle Management
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 20
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 20.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	**PSPF Core Requirements**: Classification of information; Ongoing assessment of personnel; and Entity facilities Australian Government Information Security Manual (ISM) **Legislation**: *Privacy Act 1988*
Read in conjunction with	N/A
See also DSPF Principle(s)	Security for Projects Security for Capability Planning Defence Industry Security Program Information Systems (Physical) Security Offshore and Cloud Based Computing ICT Certification and Accreditation Information Systems Log Management Information Systems Vulnerability and Patch Management Security Remote Access to Defence Systems

Implementation Notes, Resources and Tools	*Australian Government information security management guidelines – Australian Government Security Classification System* – provides guidance to assist agencies to identify the value of information and, in turn, apply a suitable protective marking. *Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and material* – provides guidance on procedures for applying protective markings and information handling procedures. *Australian Government Information Security Manual (ISM)* – sets out the standard governing the security of Australian Government ICT systems.

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	CISO	Launch

Defence Security Principles Framework (DSPF)

Information Systems Lifecycle Management

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this Enterprise-wide Control.

Escalation Thresholds

2. The ITSA has set the following general threshold for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence ITSM	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Group or Service Cyber Security Adviser **Note**: In the event that an appointment of a Group or Service Cyber Security Adviser has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Group or Service Cyber Security Executive **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Controls

System Planning

3. Defence and Defence Industry with responsibilities for projects within the Single Information Environment (SIE) are to implement approved measures to protect official information and resources in accordance with the classification of project information, systems and associated security risks. See DSPF Principle 10 –

Classification and Protection of Official Information and DSPF Principle 11 – *Security for Projects*.

4. The development and introduction of new ICT systems is to be planned in accordance with:

a. Business Impact Levels (BILs);

b. the Essential 8 ASD Strategies to Mitigate Targeted Cyber Intrusions (the top 4 of which are mandatory); and

c. applicable security architecture.

Planning and Design

5. Security is to be a fundamental consideration from the earliest stages of system planning and design.

6. All Defence systems shall have an System Sponsor and System Owner identified and documented who fully understand their security responsibilities for the systems they are responsible for.

Assessment of Business Impact Levels (BILs)

7. System Sponsors are to assess the confidentiality, integrity and availability of BILs applicable to the system being designed. These are to be communicated to the System Owner, who will also consider BILs specified by any other key stakeholders.

Protection of Design Documentation

8. System design information and documentation **must** be afforded protection in accordance with its classification, caveats and any associated BIL. Consideration is to be given to a number of factors, including:

a. the degree to which the information could highlight a vulnerability or facilitate an attack on the system (or related systems);

b. commercial sensitivity;

c. the impact of unauthorised modification to system documentation; and

d. the impact that the loss or destruction of the information would have on the ability to operate and maintain the system.

Standalone Networks

9. Standalone networks (those not connected to Defence major fixed networks) increase the complexity of managing the security of Defence ICT infrastructure. The business need for a standalone network is to be weighed against the additional

complexity of security management. CIOG is responsible for the policy and the approval of standalone networks.

Planning for Certification and Accreditation

10. System Owners are to identify the appropriate certification authority for each new system.

11. It is recommended that System Owners engage with the appropriate Certification Authority from the earliest stages of system development planning.

12. System Owners are to communicate the assessed system BIL to the Certification Authority.

13. It is recommended that System Owners identify any specific characteristics of the system that are likely to impact on certification and accreditation and discuss these with the Certification Authority at the earliest possible point. Examples might include:

a. requirements for the system to store, process or communicate foreign government information;

b. any intention to host foreign nationals on the system; and

c. any use of Industrial Control Systems (ICS) (Supervisory and Data Acquisition (SCADA), Programmable Logical Controllers (PLC) etc.

Physical Context

14. The threat environment and degree of physical protection applied to a system can have a significant impact on the system's risk profile. Considerations may include:

a. where the information/data will physically reside;

b. the system is to be deployed (including those integrated into vehicles and platforms);

c. if the system is in a mission or embassy overseas including in a High Commission Embassy or similar;

d. if the system is in an outsourced or contractor facility;

e. if the system is in a space accessible by the public; and

f. if the system supports remote access.

15. DSPF Principle 71 – *Physical Security* and DSPF Principle 30 – *Remote Access to Defence Systems* should be considered when managing the lifecycle of a system.

16. In some cases availability controls and the infrastructure used may affect risks to confidentiality or integrity. Physical certification and accreditation requirements are specified in DSPF Principle 23 – *ICT Certification and Accreditation* and DSPF Principle 73 – *Physical Security Certification and Accreditation*.

Example: *Data backups greatly reduce risks to availability, but may increase the risks to confidentiality if appropriate controls are not in place to protect backup media from theft or inappropriate access.*

17. Service providers' systems that are used to provide information technology services, including outsourced cloud services, **must** be accredited prior to handling government information. Refer DSPF Principle 21 – *Offshore and Cloud Based Computing* and DSPF Principle 23 – *ICT Certification and Accreditation*.

System Procurement

18. Responsibility for security risks cannot be outsourced and are to remain with the Group or Service responsible for the procurement.

19. CIO (or approved delegate) **must** approve any commitment of funds for procurement of any ICT hardware and/or software, including ICT infrastructure as a service or other cloud delivery models, in accordance with FINMAN2.

20. Where a Group or Service relies on an exception to this requirement as described within FINMAN2, the Sponsor **must** record their decision and the rationale within the AE643 – Defence Purchasing, and the suite of system security documentation.

21. All ICT systems, hardware and software (including those acquired without specific CIO approval) **must** be assessed and approved by the CIO before being introduced into the SIE.

22. Contract Managers are to ensure that entities to which Defence has either granted access, or entrusted with official information or assets, take appropriate precautions to safeguard the information or assets.

23. Internally developed, and commercially obtained systems, are to address security requirements as part of their:

a. initial design;

b. development;

c. testing; and

d. during future reviews and updates.

24. Procurement officers and Contract Managers are to manage the security risks that result from allowing Contractors, Consultants and Outsourced Service Providers, and their sub-contractors, access to Defence official information, ICT systems, facilities and equipment. See DSPF Principle 11 – *Security for Projects* and DSPF Principle 12 – *Security for Capability Planning*.

Defence Contracts and Procurement

25. Defence is to document requirements for information security when entering into outsourcing contracts and arrangements with Contractors, Consultants and Outsourced Service Providers. Refer DSPF Principle 21 – *Offshore and Cloud Based Computing.*

26. Security risks cannot be outsourced or transferred to Defence Industry.

Product Selection

27. When acquiring products with security features, the acquisition **must** comply with the processes outlined in the ISM Product Selection sections. If a product providing lower security functionality is selected over one that offers higher security functionality, the decision maker is to be aware of the mandated requirements, possible alternatives and the basis for the decision. The associated risk is to be documented.

28. When selecting secure products for their own use, Defence Industry is to apply the Product Selection section of the ISM.

Equipment Manager Appointment

29. An Equipment Manager is to be appointed if an ICT capability is purchased under a Defence wide support contract and is:

a. evaluated under the Evaluated Products List (EPL);

b. a Common Criteria Recognition Arrangement; or

c. a High Assurance Product (HAP).

Note: *These categories are further explained in the ISM. Hardware that implements these features will have specific ISM requirements and security measures.*

Exclusion: *Where HAP is a Controlled Cryptographic Item (CCI) or implements key material eligible for the CRYPTO caveat then DSPF Principle 13 – Communications Security (COMSEC) is the authoritative policy.*

30. The Equipment Manager is to develop a through-life support plan covering at a minimum:

a. initial purchase arrangements, including adherence to all requirements of the ISM and any security processes identified in ASD product specific advice and publications.

Note: *Where secure products apply, issues such as confirming anti-tamper mechanisms on receipt will need to be addressed. ASD provides an analysis of security issues that will need to be followed in the product's evaluation, its documentation, and other product specific advice.*

b. vulnerability and patch management guidance for which can be found in the ISM;

c. a Key Management Plan (KMP) and other cryptographic considerations (in accordance with ASD product advice);

d. asset tracking and accountability procedures;

e. maintenance arrangements including minimum personnel security requirements for individuals conducting maintenance activities; and

f. a device recall and disposal plan to ensure secure remediation or disposal when:

   i. the capability reaches its planned end of life;

   ii. devices become obsolete prior their planned end of life; or

   iii. a critical vulnerability is discovered.

System Development

System Security Documentation

31. Systems are to have relevant authorised security instructions as detailed in the ISM. Larger, complex systems may require multiple sets of documentation addressing specific aspects of the system.

Example: *In order to keep documentation manageable, a large network may have separate document sets for infrastructure, operating systems, account directories etc.*

32. Further guidance for certification / accreditation can be found in DSPF Principle 23 – *ICT Certification and Accreditation* and DSPF Principle 73 – *Physical Security Certification and Accreditation*.

Separation of Development, Test and Production Environments

33. Separate, isolated environments should be created for development, test and operational lifecycle phases.

34. Development and test environments are required to be accredited if any sensitive or classified hardware, software or information is present in the environment.

Example: *A system uses off-the-shelf hardware and software. However, firmware settings contain sensitive information and require protection.*

35. When accrediting a test or development environment, it is recommended that the following topics are considered during certification:

a. the presence of development tools and utilities not normally present in a production environment;

b. the volatility of the development environment. Development and test environments may be subject to frequent configuration changes;

c. the degree of hardening and patching applied to the development or test environment as opposed to the production environment;

d. network connectivity; and

e. data transfers to, and from, the test environment.

Physical Security During System Development

36. Systems are to be afforded adequate physical protection during each stage of development, in accordance with DSPF Principle 18 – *Information Systems (Personnel) Security*. These requirements **must** be documented in system development plans.

Security of Source Code

37. System security documentation and plans **must** identify the confidentiality, integrity and availability requirements for specific classes of source code and enact suitable protective measures.

38. A software system may be built from source code with varying levels of confidentiality requirements. Source code may be:

a. sensitive in its own right, e.g. the algorithm employed may be sensitive or classified;

b. publicly available, e.g. standard code libraries that ship with common off-the-shelf development environments; or

c. available to users, e.g. client side scripts implemented as part of a web application.

39. Consideration should be given to the degree of trust placed in third party code libraries. Specifically, does the code perform:

a. the intended action; or

b. any unwanted or unauthorised actions?

Development Standards, Architectures, and Hardening Guides

40. Defence ICT systems should be built in accordance with a Defence endorsed security architecture. Further information about system development requirements, including standards, can be found in the Software Application Development and Web Application Development sections of the ISM.

Components and Subsystems

41. Some components of a larger system may entail specific types of risks and require additional consideration.

42. Systems that use Industrial Control Systems (ICS), Supervisory and Data Acquisition (SCADA) or Programmable Logic Controllers (PLC) as subcomponents may be exposed to risks that are not applicable to other systems and therefore require additional consideration. It is recommended that any use of such components be highlighted in system design documentation and discussed with the applicable certification authority from the earliest possible stages of system development.

System Testing

43. All input to systems is to be assumed to be untrusted until verified as correct, safe and suitable.

44. System development plans are to identify the type(s) of test data to be used.

45. Test data is Defence data. It **must** be protected in accordance with assessed risks informed by a classification and/or confidentiality, integrity and availability BIL.

46. Anonymising real data **must** not allow for reversal of the process, or for identities, capabilities or limitations to be inferred

47. Plans are to give consideration to the confidentiality of test data, particularly if the data is to leave Defence control. See DSPF Principle 21 – *Offshore and Cloud Based Computing* for further requirements.

Vulnerability Assessment

48. As the ICT capability manager, CIOG is responsible for the development of a technical vulnerability assessment strategy for Defence. System Owners should consult with the relevant certification authority for advice on technical vulnerability assessments.

Introduction into Service

Certification and Accreditation

49. Defence systems are not to process official information until awarded formal accreditation in accordance with DSPF Principle 23 – *ICT Certification and Accreditation*.

50. Security accreditation only attests that the system presents an acceptable level of security risk. It does not imply compliance with any other standards or requirements.

Merging and Connecting Systems and Networks

51. System Owners are to consult with any relevant Certification and Accreditation Authorities before merging or connecting systems or networks in order to ensure that all new risks are identified and appropriately managed.

52. The user base of each system/network is to be considered in consultation with the relevant Certification Authority before they are merged or connected and appropriate controls **must** be implemented.

Note: *This is of particular importance if networks are used by foreign nationals and process information with nationality based restrictions.*

System Operation

53. ICT systems and networks are to be monitored in accordance with the requirements of DSPF Principle 19 – *Information Systems (Logical) Security.*

54. Regular reviews should be conducted to manage risks throughout the operational phase of the system's lifecycle.

System Owner Responsibilities

55. System Owners are to manage the ongoing sustainment activities throughout the systems lifecycle.

56. System Owners are to ensure the application, system, or network they are responsible for has an effective ICT Security maintenance program that covers the following essential security requirements:

a. configured and maintained end-point ICT security controls;

b. enabled and effective application white listing; and

c. up to date security pated core infrastructure software and hardware is applied.

57. System Owners are to ensure that all access controls associated with protecting classified information are periodically reviewed to ensure only authorised users have access to classified information. Reviews are to include ensuring appropriate protection methods are in place to ensure the protection of AUSTEO and foreign official information.

58. System Owners are to implement measures to control the installation of software on operational systems in accordance with the Software Security and Secure Administration sections of the ISM.

59. With regards to application whitelisting, System Owners are to ensure that users and system administrators are not permitted to temporarily or permanently disable, bypass or be exempt from application whitelisting mechanisms once enabled.

60. When patching, updating, or managing a system incident, system Owners are to manage security incidents involving systems across all phases of the incident's life cycle in order to:

a. inform understanding of Defence's security posture;

b. minimize the impact of the specific incident;

c. inform the continuous improvement of protective measures and controls; and

d. ensure that people are accountable for their actions.

61. When maintaining a system accreditation, System Owners are to ensure that all systems under their control are operated and undergo regular re-certification and re-accreditation in accordance with DSPF Principle 23 – *ICT Certification and Accreditation.*

62. When changes or updates to system configuration are proposed, system Owners are to ensure that:

a. all changes to ICT systems have successfully passed acceptance testing and received appropriate security certifications and accreditation prior to being commissioned for operational use;

Exclusion: *Where the deployment of a system change is in urgent support of a current ADF operation, direction may be issued for the change to be commissioned prior to all appropriate security certifications and accreditations being achieved. Director General Information Services (DGIS) and Director IT Services (DITS) are the sole authorities for issuing of such a direction. DGIS / DITS shall seek ITSM/ITSO advice in considering the ICT security risks associated with commissioning the proposed change for operational use prior to accreditation being achieved.*

b. all changes to configuration baselines are updated as part of the Defence Change Management process and reflect the actual configuration that was implemented under an approved change; and

c. periodic reviews of configuration baselines are conducted to ensure no unauthorised changes have been performed outside of the approved Defence Change Management process.

63. When decommissioning or disposing of systems, System Owners are to ensure that all ICT systems within the SIE are decommissioned in accordance with DSPF Principle 10 – *Classification and Protection of Official Information* and DSPF Principle 22 – *Mobility Device Security*.

User Management

64. System Owners are to ensure that all user accounts are periodically reviewed, to ensure all users are accounted for and that the appropriate level of rights have been assigned to them.

65. The management of System Users and Privileged Users, is to be performed in accordance with:

a. DSPF Principle 18 – *Information Systems (Personnel) Security*;

b. system SOPS; and

c. instructions as approved during accreditation.

System Log Management

66. System Owners are to ensure that system logs are being effectively managed throughout the life of all systems in accordance with DSPF Principle 28 – *Information Systems Log Management*.

Application Whitelisting

67. Application whitelisting **must** be enabled on ICT systems using one of the following:

a. cryptographic hashes;

b. publisher certificates;

c. absolute paths; or

d. parent folders.

68. These methods are to be applied in accordance with ISM Control numbers; 0843, 0413, 0845, 0846, 0955, 1391, 1392, 1391, 0957 and the ASD's "Essential 8 ASD Strategies relating to Application Whitelisting to prevent the execution of unapproved/malicious programs".

Note: *When enabling absolute paths, file permissions are to be configured to prevent users and system administrators from being able to modify files that are permitted to run.*

Note: *When enabling parent folders, file system permissions are to be configured to prevent users and system administrators from being able to add or modify files in the authorised parent folders*

Patching, Updating and Incident Management

69. Security patching of ICT System operating systems, applications, drivers, and hardware devices **must** be done in accordance with DSPF Principle 28 – *Information Systems Vulnerability and Patch Management Security* and ASD "Essential 8 ASD Strategies to Mitigate Targeted Cyber Intrusions" related to patching of applications.

70. Security incidents involving Defence and Defence industry information systems are to be managed in accordance with DSPF Principle 24 – *Information Systems Security Incident Management*; DSPF Principle 77 – *Security Incidents and Investigations*; and DSPF Principle 71 – *Physical Transfer of Information and Assets*.

Maintaining Accreditation

71. All changes that may impact the security of an ICT system, and are subsequently assessed as having changed the overall security risk for the system, are to result in reaccreditation.

72. Triggers for re-accreditation include significant changes to:

a. system architecture or implemented controls;

b. information stored, processed or communicated'

c. user base;

d. the environment in which the system operates; and

e. any other conditions stipulated by the accreditation authority.

Configuration and Change Management

73. All changes proposed or being considered are to have an ICT security impact analysis completed prior to being implemented to ensure security risks associated with the change have been assessed. This includes:

a. upgrades to, or introductions of, ICT equipment;

b. upgrades to, or introductions of, software; or

c. major changes to security controls including:

   i. changes in the Business Impact Levels (BILs) associated with the system (for example, the integrity of a system is reassessed or the classification raised;

   ii. significant changes to the architecture of the system or the security controls it implements;

   iii. changes to the user base of the system, particularly in regard to foreign nationals and Privileged Users; or

   iv. any other conditions stipulated by the accreditation authority.

Auditing ICT Equipment

74. The physical location of fixed ICT and electronic office equipment is to be recorded and documented. For portable ICT Assets (including Mobile devices), the custodian of the device is to be documented.

75. Auditing of ICT equipment, including electronic office equipment and networking devices, is to be performed in accordance with DSPF Principle 17 – *Information Systems (Physical) Security*.

System Maintenance

76. The security configuration of the device is not to be changed without prior authorisation via established Defence Change Management processes.

77. Where an escort is required to supervise maintenance of a classified device, the escort **must** ensure that non-volatile media is not removed from Defence custody unless the maintainer has been accredited to handle and dispose of classified material. If classified media is to be removed from the device and transferred to another person's custody, then procedures for the transfer of classified material contained in DSPF Principle 71 – *Physical Transfer of Information and Assets* are to be followed.

78. Devices containing non-volatile media are to be transferred as a classified item. For bulky equipment, non-volatile media may be removed from the device and securely transported according to its classification. A device with all non-volatile media removed has been sanitised and may therefore be transferred as an unclassified item.

Decommissioning and Disposal

Retention of Records

79. Records pertaining to a system may need to be kept after its decommissioning.

80. Investigation of a security incident suggests that classified information may have been previously compromised via a system which has since been decommissioned. Security logs from the old system may need to be audited to determine whether or not the information was compromised.

81. Event log retention requirements are specified in the ISM.

Sanitisation and Destruction of Electronic Storage Media

82. System Owners and Equipment Managers **must** document and enact processes to:

a. identify electronic storage media containing classified or otherwise sensitive information. This process is to take into account the effect of information aggregation;

Note: *When identifying electronic storage, it is important to recognise the different types of media as this can affect sanitisation and destruction requirements. In particular hybrid drives (those using a mixture of magnetic and solid state memory) have specific constraints in terms of sanitisation.*

b. Prevent media containing sensitive or classified information from being released into the public domain or disclosed through inadequate protection. This process is to meet the requirements of DSPF Principle 10 – Classification and Protection of Official Information and the ISM.

c. Record the reclassification, sanitisation or destruction of electronic storage media in a suitable register.

Disposal of Sensitive or Classified Hardware

83. Sensitive or classified hardware associated with an ICT system or electronic office equipment **must** be disposed of in accordance with accredited processes that comply with:

a. DSPF Principle 10 – *Classification and Protection of Official Information*;

b. DSPF Principle 71 – *Physical Transfer of Information and Assets*; and

c. the ISM.

84. When hardware is CCI (Controlled Cryptographic Item) or implements key material eligible for the CRYPTO caveat then it **must** be disposed of in accordance with ASD advice and all relevant ACSI documents.

Roles and Responsibilities

Chief Information Officer (CIO)

85. The CIO is responsible for:

a. providing a secure and dependable information environment;

b. ensuring the information environment is covered by suitable acceptable use policies;

c. ensuring the development and maintenance of an ICT security strategy;

d. ensuring the development and maintenance of ICT security architecture;

e. delivering an effective certification and accreditation framework for Defence that meets Government expectations;

f. developing policy and guidance on the approval to operate standalone networks;

g. developing strategies to mitigate any identified risks arising from equipment supply chains;

h. approving ICT system and equipment procurement in accordance with FINMAN2;

i. developing Defence-wide vulnerability assessment and system monitoring strategies and capabilities; and

j. providing adequate capacity to ensure the performance of the SIE.

Chief Information Security Officer (CISO)

86. The CISO is responsible for:

a. establishing the strategic direction for ICT security across Defence and Defence industry;

b. developing and maintaining an ICT security strategy;

c. contributing security expertise to the development and maintenance of an ICT security architecture;

d. maintaining an effective certification and accreditation framework for Defence and Defence industry in accordance with Government expectations, Defence policy and the Defence ICT security strategy; and

e. liaising with DS&VS and Executive Security Advisers to ensure that information systems security is integrated with broader protective security strategies, policies, and plans.

Information Technology Security Advisor (ITSA)

87. The Information Technology Security Advisor (ITSA) is responsible for:

a. coordinating ICT certification functions to a standard that meets Government expectations;

b. coordinating of Information Technology Security Managers (ITSM) across Defence in order to meet the strategic direction of the CISO;

c. liaising with ITSA in other agencies on technical ICT security matters; and

d. maintaining visibility of certified systems and any associated recommendations made to accreditation authorities.

Information Technology Security Manger (ITSM)

88. The ITSMs function is a specific subset of the System Manager role. It may be performed by the System Manager directly or the System Manager may delegate the function to a separate appointment.

89. The ITSM is responsible for:

a. liaising with the Defence ITSA;

b. informing the system manager of any identified risks to the systems for which they are responsible;

c. informing the ITSA of any risks that may also affect other systems;

d. identifying potential security improvements;

e. ensuring that security recommendations or requirements provided by the ITSA are enacted; and

f. maintaining system configuration in accordance with accredited processes.

Note: *This role has been introduced in order to align Defence terminology with the ISM. Previously within Defence, many functions of this role would have been performed by the Information Systems Security Officer (ISSO). In cases where an ISSO manages or coordinates other ISSO, the lead ISSO may become an ITSM.*

Information Technology Security Officer (ITSO)

90. With regard to the lifecycle management of information systems, the Information Technology Security Officer (ITSO) is responsible for:

a. implementing directions from the ITSM, system manager and the ITSA;

b. notifying the system manager and ITSA of any identified vulnerability that may prejudice the security of the system;

c. reporting any security incidents detected or identified; and

d. performing security management tasks in accordance with applicable SOPs and any other conditions stipulated during accreditation.

Note: *This role has been introduced in order to align Defence terminology with the ISM. Previously within Defence, many functions of this role would have been performed by the ISSO. In many cases ISSO will become ITSO.*

System Sponsor

91. System Sponsors are responsible for:

a. developing business cases that initiate the development and introduction of new systems;

b. defining system boundaries and the scope of system functions; defining the BIL of information and providing this to System Owners; and

c. securing CIO approval for ICT system and equipment procurement in accordance with FINMAN2 prior to commitment of any funds. Where an exemption is applied the decision and rational must be recorded within the AE643 - Defence Purchasing.

92. Under some circumstances, the System Sponsor may be the System Owner. Otherwise the System Sponsor will appoint a System Owner.

System Owners

93. System Owners are responsible for ensuring that:

a. the BIL of the system is informed through the information held on behalf of stakeholders;

b. systems are built and maintained to a security standard suitable for their intended use;

c. systems do not store, process or communicate official information without appropriate accreditation;

d. systems maintain accreditation;

e. systems are operated and managed in accordance with their accreditation; and

f. systems are securely decommissioned at the end of their lifecycle.

System Managers

94. System Managers are responsible for:

a. appointing a system ITSM;

> ***Note:*** *A system manager may assume the role of ITSM, depending on the size and complexity of the system.*

b. advising System Owners of any known vulnerabilities, non-compliances, unmanaged risks or other issues affecting the security of the system;

c. supporting System Owners in the development of dispensation requests as required;

d. managing and protecting system documentation;

e. making system configuration changes which are approved in accordance with defined processes;

f. monitoring and maintaining the security configuration of systems ensuring that applicable standards are met;

> ***Example:*** *Patches are tested and applied in a timely manner to maintain the standard of system security.*

g. monitoring system activity for anomalies that might indicate the realisation of a security risk; and

h. reporting any security incidents affecting the system.

Privileged Users

95. Privileged Users are only to implement changes to information systems that have:

a. been approved through a Defence Change Management process;

b. been security assessed, and any increase to the information system and/or connected systems has been accepted by the System Owner (or their delegate);

c. not introduced any significant risk that has not been duly assessed; and

d. had all baseline configuration documentation updated as part of the Defence Change Management processes, and reflect the actual configuration that was implemented under an approved change.

System Users

96. Defence personnel, Contractors, Consultants and Outsourced Service Providers are not to make any changes to information systems (including installing software/hardware or changing existing system configuration) unless they are authorised to do so in accordance with formal Defence change management processes.

Certification Authorities

97. Certification Authorities are responsible for:

a. ensuring that certification requests are supported by the necessary system documentation;

b. assessing the submitted documentation against the requirements specified in all policy and standards applicable to the system;

c. identifying areas in which the system does not comply with applicable security requirements;

d. identifying (in conjunction with the System Owner) any aspects of the system or its environment that would require controls above minimum standards;

e. communicating residual risk to the Accreditation Authority to enable an informed accreditation decision; and

f. maintaining appropriate records of certified systems and recommendations made to accreditation authorities.

Accreditation Authorities

98. Accreditation Authorities are responsible for:

a. confirming that system certification has been conducted to a suitable standard;

b. considering the residual risk (and any other associated recommendations) as communicated by the Certification Authority and deciding whether or not to accept the risks associated with operating the system;

c. documenting the decision whether or not to accredit the system in an accreditation report;

d. maintaining visibility of all systems awarded accreditation and their associated re-accreditation schedules; and

e. facilitating requests for dispensations raised by System Owners, or alternatively, notifying System Owners of the reasons for not supporting the request.

Equipment Managers

99. Equipment Managers are responsible for developing and implementing management plans for equipment throughout its lifecycle.

Key Definitions

100. **Application Whitelisting**. An approach in which an explicitly defined set of applications are permitted to execute on a given system. Any application excluded from this list is not permitted to execute.

101. **CCI**. Controlled Cryptographic Item

102. **Configuration Baseline**. The term used to describe the current approved configuration state of an information system that has been managed through Defence Change Management.

103. **Defence Change Management** is the process used to make changes to information systems baseline with the SIE.

104. **Firmware**. Software embedded in a hardware device.

105. **High Assurance Product (HAP).** A product that has been approved by ASD for the protection of information classified CONFIDENTIAL or above.

106. **Industrial Control Systems (ICS).** A class of system that controls measures or otherwise manages industrial or mechanical processes. These often represent a

boundary between logical systems and the physical world. The term ICS encompasses Supervisory Control and Data Acquisition (SCADA) systems and Programmable Logical Controllers (PLCs).

107. **Patching**. The process of applying updates to software including operating systems and applications.

108. **SAFEBASE**. Defence's protective security alert system which provides planning guidance and standards to Defence on appropriate measures to take in response to varying threat levels

Further Definitions

109. Further definitions for common DSPF terms can be found in the Glossary.

110. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Information Systems Lifecycle Management
Control Owner	Information Technology Security Advisor
DSPF Number	Control 20.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Lifecycle Management
Related DSPF Control(s)	N/A

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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Offshore and Cloud Based Computing

General principle

1. Offshore and cloud based Defence information is only hosted by cloud service providers on the 'Certified Cloud Services List' who have been evaluated and certified by the Australian Signals Directorate.

Rationale

2. Defence and Defence Industry personnel require secure access to, and communications with, information systems and electronic devices they require for work purposes.

3. Information stored offshore or in a cloud based environment is more vulnerable and subject to greater security risks than that stored in Defence or Defence Industry controlled systems and environments.

Expected outcomes

4. Technical security and business risks are managed effectively throughout each information system's life cycle. These include issues of privacy, data ownership and data sovereignty.

5. Business Impact Level assessments are used to determine the most appropriate host to be used for offshore or cloud based computing, and any arrangements are carefully considered and balanced against security risks.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	EL1/O5 employed within ICT Security Branch Integrated Risk Management (IRM) Directorate or Information Technology Security Manager (ITSM)	EL1/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	EL2/O6 employed within ICT Security Branch IRM Directorate or ITSM	EL2/O6 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive (CSE) **Note**: In the event that an appointment of a Group or Service CSE has not been made, the Defence CISO will be the appropriate escalation point
High	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor (CSA) **Note**: In the event that an appointment of a Group or Service CSA has not been made, the Defence ITSA will be the appropriate escalation point.
Extreme	Defence Chief Information Officer (CIO)	Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Offshore and Cloud Based Computing
Principle Owner	CISO
DSPF Number	21
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 21.1
Control Owner	ITSA

Related information

Government Compliance	**PSPF Core Requirements**: Classification of Information; Access to information; Safeguarding information from cyber threats; Robust information and communication technology systems. Australian Government Information Security Manual (ISM) **Legislation**: *Archives Act 1983* *Privacy Act 1988* *Freedom of Information Act 1988*
Read in conjunction with	Commonwealth Procurement Rules Foreign equivalent FOI acts Foreign operation of Foreign Intelligence Services, local intelligence collection laws Notifiable Data Breach legislation (under Privacy Act)

See also DSPF Principle(s)	Security for Projects Security for Capability Planning Foreign Release of Official Information Defence Industry Security Program Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Information Systems Data Transfer Security Information Systems Lifecycle Management Information Systems Log Management
Implementation Notes, Resources and Tools	N/A

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	CISO	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Offshore and Cloud Based Computing

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Offshore and Cloud Based Computing
Control Owner	ITSA
DSPF Number	Control 21.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Offshore and Cloud Based Computing
Related DSPF Control(s)	NA

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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Mobility Device Security

General principle

1. Defence provisioned mobility devices (including personal mobile Information and Communications Technology (ICT) e.g. phones, tablets, laptop computers etc.) are to be afforded security protections commensurate with the classification of information they process, store or communicate.

Rationale

2. Mobility devices present unique security challenges due to their:

a. rapidly evolving nature;

b. ability to capture, record, process, transmit and store large amounts of information in almost any conceivable format; and

c. ability to provide a means to exchange that information via fixed and ad-hoc networks.

Expected outcomes

3. Defence provisioned mobility devices are configured and operated in a way so that the likelihood of compromise of official information, or connected ICT systems is as low as reasonably possible.

4. Information assets are protected in order to safeguard Defence's customers, intellectual property, and reputation.

5. Security measures and practices are in place to ensure official information is protected during offsite work.

6. Defence provisioned mobility devices are protected in an appropriate manner when used outside of controlled facilities.

7. Non-Defence mobility devices are not physically connected to the Single Information Environment (SIE).

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor. **Note**: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (CIO); or Head of CIOG ICT Operations Division in the case of Accreditation matters	Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Mobility Device Security
Principle Owner	CISO
DSPF Number	22
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 22.1
Control Owner	ITSA

Related information

Government Compliance	**PSPF Core Requirements**: Safeguarding information from cyber threats; and Robust information and communication technology systems. Australian Government Information Security Manual (ISM) **Legislation:** *Privacy Act 1988 (Cth)*
Read in conjunction with	N/A
See also DSPF Principle(s)	Foreign Release of Official Information Information Systems Security Incident Management Media Protection Security Information Systems Data Transfer Security Remote Access to Defence Systems Overseas Travel Working Offsite Physical Security Security Incidents and Investigations
Implementation Notes, Resources and Tools	N/A

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	CISO	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Mobility Device Security

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise-wide Control. Mobility Device Security

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Mobility Device Security
Control Owner	ITSA
DSPF Number	Control 22.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Mobility Device Security
Related DSPF Control(s)	Foreign Release of Official Information Information Systems Security Incident Management Media Protection Security Information Systems Data Transfer Security Remote Access to Defence Systems Overseas Travel Working Offsite Physical Security 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	ITSA	Launch

Defence Security Principles Framework (DSPF)

ICT Certification and Accreditation

General principle

1. Assurance processes, ensuring appropriate protections for official information during processing, storage and communication, are applied to all Information Communications and Technology (ICT) systems and capabilities prior to their operational use.

2. Regular assessments, performed against emerging cyber threats through the Certification and Accreditation process, ensure associated risks are considered, mitigated, and/or accepted as necessary.

Rationale

3. The certification and accreditation process:

a. enables Defence to understand and manage security risks to classified information, security-protected assets and infrastructure; and

b. provides assurance that sufficient security measures are in place or, that deficiencies and their associated risks have been mitigated or accepted.

4. Accreditation of ICT systems provides other Government agencies and coalition partners with confidence that Defence Groups and Services protect shared information and security protected assets.

Expected outcomes

5. Security controls are implemented to assure the protection of information and information systems, and reduce residual risk to an acceptable and manageable level.

6. Defence liaises with the appropriate government agency to accredit and certify TOP SECRET ICT systems.

7. Appropriate physical and personnel security controls are applied and are proportionate to assessed risks.

8. ICT systems meet mandatory minimum standards before they are authorised for use.

Escalation Thresholds

Risk Rating	Responsibility	
	CIOG managed or connected systems	**Group/Service managed systems**
Low	Accreditation Authority (must be SES1/1* or above)	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation.
Moderate	Accreditation Authority (must be SES1/1* or above)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation.
Significant	Accreditation Authority (must be SES1/1* or above)	Appointed Group or Service Cyber Security Advisor (CSE). Note: In the event that an appointment of a Group or Service Cyber Security Advisor (CSA) has not been made, the Defence Information Technology Security Advisor (ITSA) will be the appropriate escalation point.
High	SES2/2*	Appointed Group or Service Cyber Security Executive Note: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point.
Extreme	SES3/3*	Appointed Group Head or Service Chief.

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	ICT Certification and Accreditation
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 23
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 23.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	**PSPF Core Requirements:** Classification of information; Access to information; Safeguarding information from cyber threats; Robust information and communication and technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Information Systems (Physical) Security Personnel Security Clearance Temporary Access Physical Security Certification and Accreditation Security Incidents and Investigations
Implementation Notes, Resources and Tools	PSPF Business Impact Levels (BIL)

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	CISO	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

ICT Certification and Accreditation

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – Certification and Accreditation Appointments

Annex B – Defence Certification and Accreditation Process

Document administration

Identification

DSPF Control	ICT Certification and Accreditation
Control Owner	Information Technology Security Adviser
DSPF Number	Control 23.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise Wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	ICT Certification and Accreditation
Related DSPF Control(s)	N/A

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	ITSA	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex A to ICT Certification and Accreditation – Certification and Accreditation Appointments

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Certification and Accreditation Appointments
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	ICT Certification and Accreditation
DSPF Number	Control 23.1

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	ITSA	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B to ICT Certification and Accreditation – Defence Certification and Accreditation Process

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document administration

Identification

DSPF Annex	Defence Certification and Accreditation Process
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	ICT Certification and Accreditation
DSPF Number	Control 23.1

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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Information Systems Security Incident Management

General principle

1. Security incidents on Defence information systems require specialist management, as they can be difficult to detect, may affect large volumes of information in short timeframes, and are not dependent on physical proximity to the targeted asset.

Rationale

2. Information Systems security incidents may affect the confidentiality, integrity or availability of Information and Communication Technology (ICT) systems. This could result in harm to Defence capabilities, resources, reputation or people.

3. The appropriate management of security incidents involving information systems is important, not only for minimising the harm caused by the incident, but also for understanding Defence's security posture and preventing similar occurrences in the future.

Expected outcomes

4. Incident management processes are pre-planned and considered as part of the ICT certification and accreditation process.

5. Defence ICT system vulnerabilities to security incidents are identified.

6. The harm caused by incidents is reduced through suitable first response processes.

7. Defence manages security incidents involving information systems across all phases of the incident's life cycle in order to:

a. minimise the impact of the specific incident;

b. inform continuous improvement of protective measures and controls;

c. inform understanding of the Defence security posture; and

d. ensure people are held accountable for their actions.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	ICT Security Branch EL1 AND reported to Chief Information Officer Group (CIOG) Defence Security Operations Centre (DSOC)	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation and reported to CIOG DSOC
Moderate	Director ICT Security Management/Defence Information Technology Security Managers (ITSM) and reported to CIOG DSOC	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation and reported to CIOG DSOC
Significant	Defence Information Technology Security Advisor (ITSA) and reported to CIOG DSOC	Appointed Group or Service Cyber Security Advisor and reported to CIOG DSOC **Note**: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO) and reported to CIOG DSOC	Appointed Group or Service Cyber Security Executive and reported to CIOG DSOC **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division) AND reported to CIOG DSOC	Appointed Group Head or Service Chief and reported to CIOG DSOC

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Information Systems Security Incident Management
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 24
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 24.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	**PSPF Core Requirements:** Classification of information; Access to information; Safeguarding information from cyber threats; Robust information and communication technology systems; Entity physical resources; and Entity facilities Australian Government Information Security Manual (ISM) **Legislation:** *Privacy Act 1988*
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Release of Official Information Physical Security Security Incidents and Investigations Escorting Security Protected or Classified Assets
Implementation Notes, Resources and Tools	N/A

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	CISO	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Security Incident Management

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Information Systems Security Incident Management
Control Owner	ITSA
DSPF number	Control 24.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Security Incident Management
Related DSPF Control(s)	Classification and Protection of Official Information Release of Official Information Physical Security Security Incidents and Investigations Escorting Security Protected or Classified Assets

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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Information Systems Business Impact Levels and Aggregation

General principle

1. Defence will protect information systems through the implementation of personnel, logical and physical security controls determined by Business Impact Level (BIL) assessments.

Rationale

2. BILs provide a consistent approach to assessing the business impacts arising from the loss or compromise of confidentiality, integrity or availability of Australian Government resources. They provide the level of detail needed to assess the business impacts for a wide range of Australian Government responsibilities and give clear, understandable definitions of business impact;

3. BILs enable consistent risk-based decisions to be made by providing a standardised measure for determining the degree of impact to Defence; and

4. BILs are especially useful when managing information security where aggregation and the distinction between BILs for confidentiality, integrity and availability need to be carefully managed to ensure appropriate security measures are applied.

Expected outcomes

5. Defence information systems and, when necessary, sub-components are categorised using BILs;

6. Defence and Defence Industry information systems that store, process or communicate official information are assigned BILs for confidentiality, integrity and availability;

7. BILs are used:

a. to determine and inform the minimum level of protection required for information systems;

b. to select and implement appropriate personnel, logical and physical security controls;

c. to inform information system certification and accreditation decisions;

d. as a primary mechanism for determining an information system's criticality rating;

8. Defence identifies information systems that have an increased likelihood of having their confidentiality, integrity and availability compromised due to:

a. the value and/or volume of information held;

b. the capability provided by the information system; or

c. the context and environment in which the information system operates; and

9. Defence will ensure additional security controls and protective measures are implemented for those information systems, as appropriate.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	Accreditation Authority (must be SES 1/1* or above)	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Accreditation Authority (must be SES 1/1* or above)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Accreditation Authority (must be SES 1/1* or above)	Appointed Group or Service Cyber Security Advisor. **Note**: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	SES 2/2*	Appointed Group or Service Cyber Security Executive **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence Chief Information Security Officer (CISO) will be the appropriate escalation point
Extreme	SES 3/3*	Appointed Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Information Systems Business Impact Levels and Aggregation
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 25
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 25.1
Control Owner	Information Technology Security Advisor

Related information

Government Compliance	**PSPF Core Requirements**: Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information ICT Certification and Accreditation Physical Transfer of Information and Assets Physical Security Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Government information security management guidelines—Australian Government security classification system – provides guidance to assist agencies to identify the value of information and in turn apply a suitable protective marking; Australian Government information security management guidelines—Protectively marking and handling sensitive and security classified information and material – provides guidance on procedures for applying protective markings and information handling procedures; and Australian Government Information Security Manual – sets out the standard governing the security of Australian Government ICT systems.

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	CISO	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Business Impact Levels and Aggregation

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control is For Official Use Only and has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common DSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Information Systems Business Impact Levels and Aggregation
Control Owner	Information Technology Security Advisor (ITSA)
DSPF Number	Control 25.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Business Impact Levels and Aggregation
Related DSPF Control(s)	Classification and Protection of Official Information ICT Certification and Accreditation Physical Transfer of Information and Assets Physical Security 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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Media Protection Security

General principle

1. Defence personnel are to ensure that all media that contains, or has contained, official information is managed appropriately to protect against unauthorised access and to protect the confidentiality, integrity and availability of the information held within.

Rationale

2. Removable media (i.e. thumb drives, DVDs, and CDs) represent unique security challenges due to its rapidly evolving nature and the ability for devices to capture, record, process and transmit large amounts of information in almost any conceivable format.

Expected outcomes

3. Defence personnel, Contractors, Consultants and Outsourced Service Providers are to ensure that all media that contains (or has processed) official, privacy, or classified information within the SIE is protected and managed in accordance with the DSPF.

4. All media used within the Single Information Environment (SIE) is to be afforded a level of protection commensurate with the classification of information they process or store and will be used in a way that will not compromise the official information or the security of Information and Communication Technology (ICT) systems.

5. The use of portable ICT assets and removable media will be risk managed in accordance with Australian Government requirements detailed in the Information Security Manual (ISM).

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor **Note**: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Advisor **Note**: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
Extreme	Chief Information Officer (CIO) (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Media Protection Security
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	26
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 26.1
Control Owner	ITSA

Related information

Government Compliance	**PSPF Core Requirements**: Access to information; Safeguarding information from cyber threats; Robust information and communication technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Foreign Release of Official Information Mobility Device Security Information Systems Security Incident Management Information Systems Data Transfer Security Remote Access to Defence Systems Overseas Travel Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Government information security guidelines – Australian Government security classification system – provides guidance to assist agencies to identify the value of information and, in turn, apply suitable protective markings. Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and materiel – provides guidance on procedures for applying protective markings and information handling procedures. Australian Government Information Security Manual – sets out the standards governing the security of Australian Government ICT systems.

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	CISO	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Media Protection Security

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Media Protection Security
Control Owner	ITSA
DSPF Number	Control 26.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Media Protection Security
Related DSPF Control(s)	Foreign Release of Official Information Mobility Device Security Information Systems Security Incident Management Information Systems Data Transfer Security Remote Access to Defence Systems Overseas Travel 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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Information Systems Data Transfer Security

General principle

1. Defence and Defence industry are to ensure that official information is transferred in a secure manner and are only received by the intended recipient.

Rationale

2. Defence needs to regularly transfer official information, security protected and classified assets to Defence and non-Defence locations both in Australia and overseas with secure means of transfer to reduce the risk of loss or compromise.

Expected outcomes

3. Data is shared in accordance with agreements or arrangements between the parties concerned.

4. Information is protected during its transfer.

5. The ‘need to know’ principle is considered in conjunction with the ‘need to share’ principle before transferring any information.

6. The security measures required to protect classified information and security-protected assets during transfer are determined.

7. Data transfers are accomplished via Information and Communication Technology (ICT) systems wherever possible.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Executive
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security. Executive
Extreme	Chief Information Officer (CIO)(responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Information Systems Data Transfer Security
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 27
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 27.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	**PSPF Core Requirements**: Access to Information, and Safeguarding Information from Cyber Threats. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Security for Projects Foreign Release of Official Information Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Offshore and Cloud Based Computing
Implementation Notes, Resources and Tools	N/A

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	CISO	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Data Transfer Security

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise-wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Information Systems Data Transfer Security
Control Owner	Information Technology Security Advisor (ITSA)
DSPF Number	Control 27.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Data Transfer Security
Related DSPF Control(s)	Classification and Protection of Official Information Security for Projects Foreign Release of Official Information Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Offshore and Cloud Based Computing

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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Information Systems Log Management

General principle

1. Defence must develop and implement an event logging strategy covering logging facilities, including availability requirements and the reliable delivery of event logs to secure centralised logging facilities.

Rationale

2. Logging events from critical systems, applications and services within the single information environment can help detect, attribute and respond to compromise. It also supports accountability.

Expected outcomes

3. Defence systems are configured to enable sufficient logging and audit capabilities to detect cyber security incidents, attempted intrusions and unusual usage patterns that are protected from modification and unauthorised access, and whole or partial loss within the defined retention period; and

4. Defence is to retain event logs for a minimum of 7 years in accordance with the National Archives of Australia's (NAA) Administrative Functions Disposal Authority.

Escalation Thresholds

5. The Information Technology Security Advisor (ITSA) has set the following general threshold for risks managed against this *Defence Security Principles Framework (DSPF) Enterprise-wide Control* and the related *DSPF Principle and Expected Outcome*.

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	Information and Communication Technology (ICT) Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Advisor **Note**: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (CIO) (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Appointed Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Information Systems Log Management
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 28
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 28.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	**PSPF Core Requirements**: Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems. *Australian Government Information Security Manual (ISM)* **Legislation**: *Archives Act 1983*
Read in conjunction with	N/A
See also DSPF Principle(s)	Information Systems (Logical) Security ICT Certification and Accreditation Information Systems Security Incident Management Security Incidents and Investigations
Implementation Notes, Resources and Tools	*Australian Government information security management guidelines – Australian Government security classification system* – provides guidance to assist agencies to identify the value of information and, in turn, apply a suitable protective marking *Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and material* – provides guidance on procedures for applying protective markings and information handling procedures *Australian Government Information Security Manual* – sets out the standard governing the security of Australian Government ICT Systems

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	CISO	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Information Systems Log Management

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise-wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document administration

Identification

DSPF Control	Information Systems Log Management
Control Owner	ITSA
DSPF Number	Control 28.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Log Management
Related DSPF Control(s)	Information Systems (Logical) Security ICT Certification and Accreditation Information Systems Security Incident Management 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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Information Systems Vulnerability and Patch Management

General Principle

1. Defence will monitor newly identified Information and Communications Technology (ICT) vulnerabilities, prioritise patch deployment activities and develop appropriate risk mitigation strategies for Defence information systems that are unable to be patched within the specified timeframes.

Rationale

2. Security Patch Management is a critical aspect of maintaining the integrity of information systems. Security updates, or patches, are published by vendors to remediate identified vulnerabilities in operating systems, applications, firmware, and device drivers. Timely application of security updates is important and effective processes to protect Defence ICT systems from known vulnerabilities.

Expected Outcomes

3. Defence assets are monitored for vulnerabilities, and likelihood of threats and impact which are documented and used to determine risks.

4. Processes are established to receive, analyse and respond to vulnerabilities disclosed to Defence from internal and external sources (e.g. internal testing, security bulletins, security researchers).

5. Management plans are developed and implemented, and scans are performed in order to detect vulnerabilities.

6. Newly identified vulnerabilities are mitigated within the stated timeframes of the ISM, unless granted a deferral for non-compliance.

7. Defence develops remediation strategies for unpatched system vulnerabilities.

Risk Rating	Responsibility	
	Chief Information officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	ICT Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation
Moderate	Director ICT Security Management/Defence ITSM	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation
Significant	ITSA	Appointed Group or Service Cyber Security Adviser. **NB:** In the event that an appointment of a Group or Service Cyber Security Adviser has not been made, the Defence ITSA will be the appropriate escalation point
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive **NB:** In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point
Extreme	Chief Information Officer (responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Information Systems Vulnerability and Patch Management
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 29
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 29.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	**PSPF Core Requirements**: Classification of information; Access to information; Safeguarding information from cyber threats; and Robust information and communication technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Security for Capability Planning Defence Industry Security Program Offshore and Cloud Based Computing ICT Certification and Accreditation Information Systems Security Incident Management Security Incidents and Investigations
Implementation Notes, Resources and Tools	• Australian Government Information security management guidelines – Australian Government security classification system – provides guidance to assist agencies to identify the value of information and, in turn, apply a suitable protective marking • Australian Government information security management guidelines – Protectively marking and handling sensitive and security classified information and material – provides guidance on procedures for applying protective markings and information handling procedures • The Australian Government Information Security Manual (ISM) assists in the protection of information that is processed, stored or communicated by Defences' systems • The Strategies to Mitigate Cyber Security Incidents complements the advice in the ISM • The Essential Eight Maturity Model complements the advice in the Strategies to Mitigate Cyber Security Incidents

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	CISO	Launch

Defence Security Principles Framework (DSPF)

Information Systems Vulnerability and Patch Management

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise-wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Information Systems Vulnerability and Patch Management
Control Owner	Information Technology Security Advisor (ITSA)
DSPF Number	Control 29.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-Wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Information Systems Vulnerability and Patch Management
Related DSPF Control(s)	Security for Capability Planning Defence Industry Security Program Offshore and Cloud Based Computing ICT Certification and Accreditation Information Systems Security Incident Management 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	ITSA	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Remote Access to Defence Systems

General principle

1. Defence will ensure there are appropriate security controls on the use of remote access to prevent unauthorised access to Defence information.

Rationale

2. Defence personnel, Contractors, Consultants and Outsourced Service Providers may be required to work offsite. While remote access capabilities give users the flexibility to perform their duties away from the office (refer to DSPF Principle 70 – *Working Offsite*), appropriate controls need to be in place to prevent the technical compromise of official information.

Expected outcomes

3. The provision of remote access services is limited to authorised Defence personnel, Contractors, Consultants and Outsourced Service Providers, with authorisation from the relevant authority to do so.

4. Remote access users are made aware of their responsibilities to protect official information when conducting Defence work offsite.

5. Users requiring remote access are provided this through approved systems.

Escalation Thresholds

Risk Rating	Responsibility	
	Chief Information Officer Group (CIOG) managed or connected systems	**Group/Service managed systems**
Low	Information and Communication Technology (ICT) Security Branch EL1	EL1/O4 employed in a relevant Group/Service Cyber/ICT security organisation.
Moderate	Director ICT Security Management/Defence Information Technology Security Manager (ITSM)	EL2/O5 employed in a relevant Group/Service Cyber/ICT security organisation.
Significant	Defence Information Technology Security Advisor (ITSA)	Appointed Group or Service Cyber Security Advisor. **Note**: In the event that an appointment of a Group or Service Cyber Security Advisor has not been made, the Defence ITSA will be the appropriate escalation point.
High	Defence Chief Information Security Officer (CISO)	Appointed Group or Service Cyber Security Executive **Note**: In the event that an appointment of a Group or Service Cyber Security Executive has not been made, the Defence CISO will be the appropriate escalation point.
Extreme	Chief Information Officer (CIO)(responsibility as Accreditation Authority is delegated to Head of CIOG ICT Operations Division)	Group Head or Service Chief

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Remote Access to Defence Systems
Principle Owner	Chief Information Security Officer (CISO)
DSPF Number	Principle 30
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 30.1
Control Owner	Information Technology Security Advisor (ITSA)

Related information

Government Compliance	**PSPF Core Requirements**: Safeguarding information from cyber threats; Classification of Information; and Robust information and communication technology systems. Australian Government Information Security Manual (ISM)
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Security for Projects Information Systems (Physical) Security Information Systems (Personnel) Security Offshore and Cloud Based Computing Overseas Travel Working Offsite
Implementation Notes, Resources and Tools	• Australian Government Information Security Manual – sets out the standard governing the security of Australian Government ICT systems • Defence Remote Electronic Access & Mobility Service (DREAMS)

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	CISO	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Remote Access to Defence Systems

Control Owner

1. The Information Technology Security Advisor (ITSA) is the owner of this enterprise-wide control.

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control

2. This section of this DSPF Enterprise-wide Control has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Remote Access to Defence Systems
Control Owner	Information Technology Security Advisor (ITSA)
DSPF Number	Control 30.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Remote Access to Defence Systems
Related DSPF Control(s)	Classification and Protection of Official Information Security for Projects Information Systems (Physical) Security Information Systems (Personnel) Security Offshore and Cloud Based Computing Overseas Travel Working Offsite

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	ITSA	Launch

Defence Security Principles Framework (DSPF)

Personnel Security Clearance

General principle

1. Only those people recognised as eligible, suitable and trusted will obtain and retain access to Australian Government resources (people, information and assets).

Rationale

2. An assured and trusted workforce of security cleared personnel is a critical protective security control. It underpins the effectiveness of many other controls and efficient business practices.

Expected outcomes

3. The Australian Government Security Vetting Agency (AGSVA) will conduct personal security vetting for Defence personnel, Contractors, Consultants and Outsourced Service Providers.

4. In accordance with the Protective Security Policy Framework (PSPF), the personal security vetting process will be used to assess the eligibility and suitability of an applicant to hold and maintain a clearance.

5. Defence, Government, industry and foreign partners will confidently give access to classified information and assets to Defence personnel, Contractors, Consultants, and Outsourced Service Providers holding a security clearance.

6. Security clearance holders, managers and security officers will report: changes of circumstances; suspicious, ongoing, unusual or persistent contact; and any other significant incidents which may impact on the clearance holder's suitability to hold a clearance.

Escalation Thresholds

7. Departure from PSPF policy requirements.

Risk Rating	Responsibility
Low	Assistant Secretary Vetting (ASV) or authorised delegate
Moderate	ASV
Significant	Defence Security Committee (DSC) – through ASV
High	DSC – through ASV
Extreme	Will not be accepted. Must treat, including by avoiding the risk (i.e. ceasing the relevant activity)

8. Approval or changes to Eligibility Waivers.

Risk Rating	Responsibility
Low	Group Head/Service Chief or authorised delegate
Moderate	Group Head/Service Chief or authorised delegate
Significant	Group Head/Service Chief or authorised delegate
High	Secretary – through First Assistant Secretary Security and Vetting Service (FAS S&VS)
Extreme	Will not be accepted. Must treat, including by avoiding the risk (i.e. ceasing the relevant activity)

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Personnel Security Clearance
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	40
Version	2
Publication date	20 June 2019
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 40.1
Control Owner	Assistant Secretary Vetting (ASV)

Related information

Government Compliance	**PSPF Core Requirements:** Eligibility and suitability of personnel; Ongoing suitability and management of personnel; and Separating personnel **Legislation:** *Privacy Act 1988 (Cth)* *Freedom of Information Act 1982 (Cth)* *Public Service Act 1999 (Cth)* *Australian Citizenship Act 2007 (Cth)*
Read in conjunction with	DSPF Governance and Executive Guidance DSPF Controls, Processes and Instructions PSPF Mandatory Requirements
See also DSPF Principle(s)	Classification and Protection of Official Information Information Systems (Personnel) Security Contact Reporting Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	• Australian Government personnel security protocol • Australian Government personnel security guidelines – Vetting Practices • Australian Government, Protective security better practice guide • Military Personnel Policy Manual

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	20 June 2019	FAS S&VS	PSPF alignment update

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Personnel Security Clearance

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The Assistant Secretary Vetting (ASV) is responsible for the application of enterprise personnel security vetting.

Control

2. This section of this DSPF Enterprise-wide Control is For Official Use Only and has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further definitions

3. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Personnel Security Clearance
Control Owner	Assistant Secretary Vetting (ASV)
DSPF Number	Control 40.1
Version	2
Publication date	20 June 2019
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Personnel Security Clearance
Related DSPF Control(s)	Classification and Protection of Official Information Information Systems (Personnel) Security Contact Reporting Access Control 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	ASV	Launch
2	30 June 2019	ASV	PSPF alignment update

Defence Security Principles Framework (DSPF)

Temporary Access to Classified Information and Assets

General principle

1. For urgent operational or business needs, people without the necessary security clearance may be granted limited and controlled, temporary access to classified information and assets. The approval of such access does not constitute the granting of a security clearance.

Rationale

2. Access to security classified information and assets requires individuals to have an appropriate clearance and a need to-know.

3. If an individual requires access for legitimate reasons, that access may be granted on a temporary, limited and controlled basis.

Expected outcomes

4. Temporary access to security classified resources is only approved for urgent operational or business reasons, not as a substitute for sound personnel security management or appropriate workforce planning.

5. Temporary access provisions are only used for situations that involve access to security classified information or assets.

6. Defence does not provide temporary access to caveat, CODEWORD or compartmented information at any classification.

7. Temporary access is strictly supervised and confined to information or assets that are essential to the requirement for which the temporary access was approved.

8. Temporary access to ICT networks is not approved unless it can be strictly confined to information that is essential to operational or business needs.

9. Any misuse of temporary access provisions, unauthorised access, or conflicts of interest are reported as security incidents.

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 Security Policy and Services (AS SPS)
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Temporary Access to Classified Information and Assets
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 41
Version	2
Publication date	31 March 2019
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 41.1
Control Owner	Assistant Secretary Policy and Services (AS SPS)

Related information

Government Compliance	**PSPF Core Requirements**: Security governance for contracted service providers; Security governance for international sharing; Classification of information; Access to information; Safeguarding information from cyber threats; Robust information and communication technology systems; and Eligibility and suitability of personnel. **Legislation**: *Members of Parliament (Staff) Act 1984 (Cth)* *Privacy Act 1988 (Cth)* *Freedom of Information Act 1982 (Cth)*
Read in conjunction with	Australian Government Security Classification System (AGSCS)
See also DSPF Principle(s)	Classification and Protection of Official Information Foreign Release of Official Information Defence Industry Security Program Personnel Security Clearance Identity Security Physical Transfer of Information and Assets Physical Security Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Security Intelligence Organisation (ASIO), Security Equipment Guides (SEGs) are available from the GovDex Protective Security Community. Information Security Manual (ISM) Control 0441

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 March 2019	FAS S&VS	Foundational review; PSPF update; and security classification alignment

Defence Security Principles Framework (DSPF)

Temporary Access to Classified Information and Assets

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner for this Enterprise-wide Control.

Escalation Thresholds

2. The AS SPS has set the following general thresholds for risks managed against this DSPF Control and the related DSPF Principle and Expected Outcomes.

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 SPS
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Controls

Temporary Access

3. Temporary access allows limited, supervised access to specific security classified information and assets to meet an operational or business need. Commanders and Managers are to supervise and monitor the information and assets accessed under these arrangements.

4. Temporary access is to be strictly confined to the specific security classified information or assets required to meet the operational or business need. An inability to accurately identify and record the specific classified documents, files or assets that will be accessed not only limits the ability to conduct a risk assessment, but suggests that unrestricted access is required and hence the use of Temporary access provisions is inappropriate. In these circumstances, a clearance should be sought for Ongoing access.

5. Temporary access is not a security clearance. It cannot be used instead of a security clearance other than to provide assurance for access to specific security classified assets (information or physical).

Note: *some individuals may work in positions of high responsibility, and may have delegations and duties that, if mishandled or abused, could cause Defence considerable harm or reputational damage. These may include personnel whose duties require them to have wide-ranging, highly discretionary access that provides them with the ability and opportunity to cause extensive harm, particularly where the potential for undetected wrongdoing is high or may take significant time to become evident. Defence policy requires that these positions are identified as Designated Security Assessment Positions (DSAP) and the occupant holds an appropriate Australian Government security clearance.*

Example: *Defence policy mandates that Defence personnel hold a minimum security clearance of Negative Vetting level 1 (NV1) prior to having independent access to bulk weapons. Temporary access cannot be used to satisfy this requirement.*

Example: *A Defence employee requires an NV1 to be allowed unescorted access to a security zone within a building. Temporary access is not a security clearance and therefore cannot be used to allow access to the security zoned area.*

Temporary Access, Caveats, DLM and Need-to-Know

6. Access to information requires that a person has a ‘need-to-know’ and the appropriate security clearance. Temporary access provisions only address security clearance requirements, they do not alter a person’s need-to-know.

7. The approval of Temporary access cannot alter the effect of caveats. Approved Temporary access does not grant access that would otherwise be limited by caveats.

Note: *The Australian Government Protective Security Policy Framework (PSPF) prohibits the use of Temporary access provisions to enable access to Caveat, CODEWORD, or Compartmented information.*

Example: *An Australian Defence Force member has a current Negative Vetting level 2 clearance and is in the process of upgrading to Positive Vetting (PV). Temporary access provisions cannot be used to grant this individual Temporary access to Caveated, CODEWORD, or Compartmented information.*

Types of Temporary Access

8. There are two types of Temporary access 'Short Term' and 'Provisional' for managing limited access to classified information and resources. Each type of access encompasses specific limitations and prerequisites. See PSPF - 9 Access to information.

Note: *The Defence Security Manual (DSM) previously specified three types of Temporary access; Limited Higher Access, Emergency Access and Provisional Access. This has been reduced to the two types of Temporary access as described above in order to align with the PSPF.*

Requirements and Constraints on Temporary Access

9. Temporary access will only be approved when there is no other current clearance holder available that can carry out the duties required. If a current clearance holder is available, but cannot carry out the duties, this will be documented in the risk assessment and be considered by the approving authority.

10. In addition to limitations applied within PSPF - 9 Access to information, Temporary access:

a. is not to be approved:

   i. to permit access to any material classified TS unless the person requiring the access holds an Australian Government Negative Vetting level 1 clearance;

   ii. retrospectively to avoid managing a security incident resulting from unauthorised or incidental access to classified material; or

   iii. if the clearance holder has been subject to an adverse security clearance decision at the level of the requested Temporary access, or is currently under review for cause (e.g., clearance downgraded due to security concerns, or higher level clearance previously denied on security grounds.)

b. Temporary access is only to be approved:

   i. by Defence Personnel. Defence industry cannot approve Temporary access on behalf of the Australian Government; and

   ii. if the scope of the approved information access can be defined and the ownership of the information is understood.

11. Temporary access is only available to persons who either currently hold, or are eligible to be considered for, an Australian Government security clearance.

12. Temporary access is not available to foreign nationals who hold a foreign government security clearance that is recognised through a Security of Information Agreement/Arrangement (SIA).

Example: *A foreign national has a recognised clearance that allows them to see PROTECTED material. As they have a recognised foreign clearance, they cannot be approved for Temporary access to SECRET material.*

13. If a foreign national has been granted an Australian Government security clearance on the basis of successfully approved eligibility waivers, they may be considered for Temporary access if required (this does not include Temporary access to Top Secret (TS) information.)

14. The approval of Temporary access does not permit unrestricted access to Defence ICT networks. If Temporary access is required to ICT resources, Information Security Manual (ISM) *control 0441* requires that the account holder's access is either restricted to only the information that is required for the specified duties, or is continually supervised by another user who has the appropriate security clearance to access the system.

15. Normal user access on systems such as the Defence Protected Network (DPN) and Defence Secret Network (DSN) grant access to very large volumes of information on web sites and shared drives, the risk of granting access to this material is accepted for those with a security clearance at the required level, but is considered too great for those that have not completed the security clearance process. Therefore if unrestricted ICT access is required, approval is to be processed as a minimum of SIGNIFICANT risk for the DPN and as a minimum of HIGH risk for the DSN, or similarly classified networks, before access is granted.

Members of Parliament (Staff) Act 1984 (MOPS Act) Staff

16. For information regarding the granting of Temporary access to MOPS Act staff, see PSPF - 9 Access to information.

Approval Authorities

17. The following table identifies the approving authorities for Temporary access.

Table 1 – Authority to Approve Temporary Access

Access To	Type of Temporary Access	
	Short Term	**Provisional**
Information requiring a PV as a prerequisite to access	Unavailable	Unavailable
Caveat / CODEWORD / Compartmented material of any classification	Unavailable	Unavailable
TOP SECRET excluding CODEWORD (refer Note 1)	Group Head, Service Chief or approved delegate in consultation with AGSVA	Minimum of SES Band 1/O-7 (or approved delegate) in consultation with AGSVA SADFO (only for SAFEBASE related emergencies)
SECRET and below excluding CODEWORD	Commander, Manager or Contract Manager in consultation with AGSVA Senior Australian Defence Force Officer (SADFO) (only for SAFEBASE related emergencies)	

18. TOP SECRET excluding Caveat, CODEWORD and Compartment - Note 1**:** Clearance subjects are to hold an Australian Government security clearance at minimum of Negative Vetting level 1 for access to this level of material under Temporary access arrangements. For *MOPS Act* staff, see PSPF - 9 Access to information.

Note: *Chief Joint Operations (CJOPS) discharges these responsibilities in respect of personnel on overseas operations.*

Processing Temporary Access Requests

19. The area approving Temporary access will assess the risks associated with doing so, specify risk monitoring requirements and identify the responsible appointment. The assessment of risk is to be in accordance with PSPF - 9 Access to information.

20. The Commander or Manager (or their delegate) of the area seeking Temporary access for an employee are to:

a. prior to processing a request for Temporary access, consult with AGSVA (and the Department of Finance in relation to MOPS Act staff) to determine if an applicant for Temporary access has any pre-existing clearance conditions or restrictions recorded on their Personnel Security File that would prevent Temporary access from being approved. This consultation should be initiated through the Security Officer of the requesting area;

b. consult with other areas in Defence and/or other agencies if the Temporary access will result in access to their information;

c. prepare and staff a business case requesting Temporary access from the appropriate authority (refer Table 1 – Authority to Approve Temporary Access);

d. make the decision to deny or approve requests for Temporary access for which they are the nominated delegate;

e. formalise the arrangement in writing with the applicant, including advising the applicant of the information that can be accessed under these arrangements and their responsibilities with regard to confidentiality and the protection of the information;

f. record the details of access in the security register;

g. ensure ongoing monitoring of approved Temporary access to ensure that it is strictly confined to the identified information and assets essential to the operational and business need for which the access was approved;

h. report any inappropriate or unauthorised access as a security incident in accordance with DSPF Principle 77 – *Security Incidents and Investigations*; and

i. review the duties and responsibilities of the position and, if required:

   i. upgrade the position's security clearance requirement; and

   ii. initiate a security clearance upgrade for the individual.

Note: *Contract Managers discharge these responsibilities in respect of the Contractors, Consultants and Outsourced Service Providers they manage.*

21. If the steps in the above paragraphs cannot be performed due to the urgent and immediate requirement to grant access in an emergency situation these steps are to be undertaken as soon as is practical following the granting of Temporary access.

Temporary Access Denied

22. Temporary access decisions are not final security clearance decisions. They are based on incomplete information that does not allow for a full assessment of the person. Any decision not to grant, or to withdraw, Temporary access does not indicate that a person will necessarily be found unsuitable to hold a security clearance by the AGSVA, even if AGSVA has identified concerns during the application for Temporary access. Subsequent investigation by AGSVA during the full security clearance process may identify mitigating factors or reveal new information.

Key Definitions

23. **Australian Government Security Vetting Agency**: AGSVA is a branch of the Defence Security and Vetting Service (DS&VS) that provides independent security clearance vetting services and advice to non-exempt government agencies (including Defence.)

24. **MOPS Act staff**: Staff employed by an Australian Government Minister under the *Members of Parliament (Staff) Act 1984 (Cth)*.

25. **Ongoing access**: Access to classified information or assets for longer than three months, or regular access for shorter periods, constitutes Ongoing access. This requires an individual to have the appropriate security clearance and a need-to-know.

26. **Temporary access**: A temporary arrangement that in specified circumstances provides limited access to security classified information to people who are yet to be issued with an appropriate security clearance. There are two types of Temporary access: Provisional access and Short Term access.

27. **Provisional access**: A form of Temporary access that can be approved after a person submits all information required for a security clearance, but before the clearance is finalised, to allow that person to access security classified information on a limited basis only.

28. **Short Term access**: A form of Temporary access used where access to security classified information is required by a person who does not have the appropriate security clearance.

29. **Limited Higher Access (obsolete term):** This term refers to an older form of Temporary access and should no longer be used, except when referring to old arrangements.

30. **Emergency Access (obsolete term):** This term refers to an older form of Temporary access and should no longer be used, except when referring to old arrangements.

Further Definitions

31. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Temporary Access to Classified Information and Assets
Control Owner	Assistant Secretary Security Policy and Services
DSPF Number	Control 41.1
Version	2
Publication date	31 March 2019
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Temporary Access to Classified Information and Assets
Related DSPF Control(s)	Classification and Protection of Official Information Foreign Release of Official Information Defence Industry Security Program Personnel Security Clearance Identity Security Physical Transfer of Information and Assets Physical Security Access Control 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	02 July 2018	AS SPS	Launch
2	31 March 2019	AS SPS	Foundational review; PSPF update; and security classification alignment

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, Contractors, Consultants and Outsourced Service Providers 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, Contractors, Consultants and Outsourced Service Providers report all such unauthorised disclosures as a security incident.

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: *Contractors, Consultants and Outsourced Service Providers 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 Security and Vetting Service (FAS S&VS)
DSPF Number	42
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 42.1
Control Owner	AS PPEC

Related information

Government Compliance	**PSPF Core Requirements**: Entity physical resources; and Eligibility and suitability of personnel. **Legislation**: *ASIO Act 1979*, Part V section 92 *Crimes Act 1914*, Part IAC Assumed Identities *Intelligence Services Act 2001*, Part 6, section 41 *Defence (Inquiry) Regulations 1985*
Read in conjunction with	Verification of Identities will be addressed by Defence People Group's Identity Management Framework in 2018. Controls surrounding Protected Identities are addressed in DSPF Control 42.1 – *Protected Identities*
See also DSPF Principle(s)	Classification and Protection of Official Information Information Systems (Personnel) Security ICT Certification and Accreditation Personnel Security Clearance Overseas Travel Physical Security Certification and Accreditation Security Incidents and Investigations
Implementation Notes, Resources and Tools	Defence People Group's 'Identity Management Framework' Defence Form XP168 - Report of Security Contact Concern. Defence process for granting honours and awards (including the process for individuals with protected identities). Defence 06.1.4 The Administrative Inquiries Manual, Chapter 7: scoping and planning a Court of Inquiry. National Identity Security Strategy 2012. National Identity Proofing Guidelines 2014.

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 SPS	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Protected Identities

Redacted Version: *Classified content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. Assistant Secretary People Policy and Employment Conditions (AS PPEC) is the Control Owner for this control under the Administration & Governance Domain of the Administrative Policy Framework (which includes Security). The Associate Secretary is the Accountable Officer for this domain. The First Assistant Secretary Security and Vetting Service (FAS S&VS) is the Policy Owner for security.

Control

2. This section of this DSPF Enterprise-wide Control is classified and has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. 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*.

Document administration

Identification

DSPF Control	Protected Identities
Control Owner	AS PPEC
DSPF Number	Control 42.1
Version	1
Publication date	2 July 2018
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 Systems (Personnel) Security 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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex A to Protected Identities – Process For Granting Honours and Awards

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The Assistant Secretary People Policy and Employment Conditions (AS PPEC) is the owner of this enterprise-wide annex.

Control

2. This section of this DSPF Enterprise-wide Annex is For Official Use Only and has been removed from this version. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document administration

Identification

DSPF Annex	Protected Identities
Annex Version	1
Annex Publication Date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identity Security
DSPF Number	Control 42.1

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	CJLOG	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Overseas Travel

General principle

1. Defence seeks to protect its people and information from threats or loss arising from official or private overseas travel.

Rationale

2. Travel to overseas countries may expose Defence personnel, Contractors, Consultants and Outsourced Service Providers to threats which could compromise national security and personal safety. These threats may not be present in Australia and thus not familiar to travellers. Due to this, it is crucial that travellers are briefed before travel to raise awareness of their destinations security environment, and ensure adequate precautions are taken.

Expected outcomes

3. Defence personnel, Contractors, Consultants and Outsourced Service Providers are to notify the relevant Department authorities of their travel plans in a timely manner.

Note: *Certain countries, including the United States of America and Canada, have moratoriums and minimum lead times for processing official travel visit requirements. DS&VS International Visits Office (IVO) can be contact for further advice.*

4. For official travel, it is expected that the traveller:

a. discusses applicable limitations and requirements with their Security Officer;

b. if a Sensitive Compartmented Information (SCI) access holder, report proposed travel to the compartment owner via Australian Signal Directorate Security or Communications Intelligence Security Officer (COMSO);

c. be aware of any relevant security risks as advised by the Security Officer, COMSO or sponsor for official travel, this includes, but is not limited to:

   i. the traveller's personal safety;

ii. the traveller's requirement to protect official information; or

iii. cultivation by Foreign Intelligence Services (FIS).

d. be aware of their responsibilities to protect official information;

e. report any suspicious contact, security incidents or any other security concern to DS&VS upon their return; and

Note: *this can be done by submitting a security incident or contact report online.*

f. ensures that visits to allied facilities are conducted in accordance with our bilateral security responsibilities and the business processes of the hosting country. More information can be found on the Overseas Travel and Visits webpage.

5. For private travel, it is expected that the traveller:

a. completes an AB644 Overseas Travel Briefing and Debriefing form as soon as possible after identifying the need to travel;

b. (if Australian Defence Force (ADF)), adheres to the restrictions as per the Pay and Conditions Manual (PACMAN) Chapter 5, Part 2, Division 1 Restricted Destination;

c. (if Australian Public Service (APS)), discusses applicable limitations and requirements with their Security Officer;

d. (if a SCI access holder), reports proposed travel to the compartment owner and is informed of any relevant security risks as advised by the Security Officer or COMSO, which includes but are not limited to:

i. traveller personal safety;

ii. official information; or

iii. cultivation by Foreign Intelligence Services (FIS).

e. if a holder of a positive vetting clearance, must use their Australian passport unless granted specific permission to do otherwise; and

f. report any suspicious contact, security incidents or any other security concern to DS&VS. Members of Defence Intelligence Agencies (DIAs) should also notify ASD Security during their debrief.

Note: *this can be done by submitting a security incident or contact report online.*

6. Defence personnel, Contractors, Consultants and Outsourced Service Providers are not to make false declarations regarding their employment. When required, the traveller is to list their status as “government employee” or “contractor”.

Escalation Thresholds

Add content

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 Security Policy and Services (AS SPS)
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Overseas Travel
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 44
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 44.1
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)

Related information

Government Compliance	**PSPF Core Requirements**: Eligibility and suitability of personnel; and Ongoing assessment of Personnel. **Legislation:** *ASIO Act 1979 (Cth)* *Work Health and Safety Act 2011 (Cth)*
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Foreign Release of Official Information Contact Reporting Physical Transfer of Information and Assets Security Incidents and Investigations
Implementation Notes, Resources and Tools	DFAT Smartraveller Security forms and tools available on the Security Portal: 1. Notification of Proposed Overseas Travel (form AB644) 2. Defensive Briefing Before Overseas Travel 3. Certification of Security Advice Given for Overseas Travel 4. Overseas Travel – Debriefing Certificate (AB645) Overseas Visit Authority (form AA 062) DSN country-specific threat advice Security of Information Agreements and Arrangements (SIAs) Defence Intelligence Security (DIS)

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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Overseas Travel

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the Control Owner for this Enterprise-wide Control.

Escalation Thresholds

2. The AS SPS has set the following general thresholds for risks managed against this Defence Security Principles Framework (DSPF) Control, and related Principle and Expected Outcome.

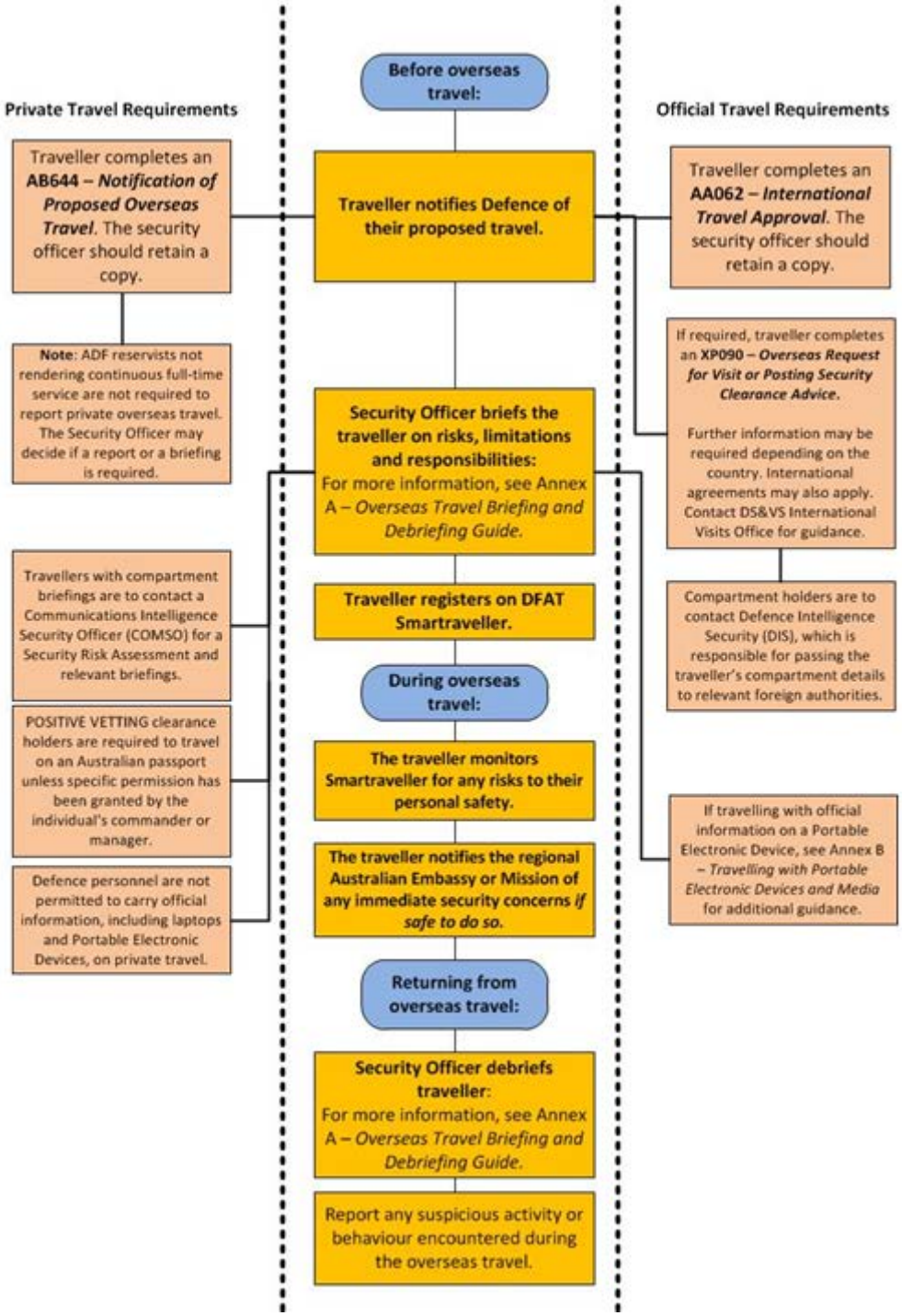
Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	AS SPS
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

3. Figure 1 outlines the Overseas Travel security process.

Note: *The AA062 - International Travel Approval form is currently under development and will be available soon. For all official travel, please use the AB644 - Notification of Proposed Overseas Travel form*

Figure 1 – Overseas Travel Security Process



Roles and Responsibilities

DS&VS International Visits Office, Australian Signals Directorate Security and Executive Security Advisers

4. The International Visits Office (IVO) of the Defence Security & Vetting Service (DS&VS), Australian Signals Directorate (ASD) Security and the Executive Security Advisers (ESA) of the Services are responsible for the provision of advice regarding overseas travel security compliance requirements.

5. The IVO is also responsible for passing security clearance details of Defence personnel, Contractors, Consultants and Outsourced Service Providers to foreign governments.

6. ASD Security is the compartment sponsor of Defence personnel, Contractors, Consultants and Outsources Service Providers, and is responsible for passing the details of a travelling individual's Sensitive Information Compartments (SIC) (if held) to foreign governments.

Commanders and Managers

7. Commanders and Managers are responsible for processing and approving all overseas travel requests and ensuring that all Defence personnel, Contractors, Consultants and Outsourced Service Providers travelling overseas are aware of their security responsibilities in accordance with the DSPF.

Security Officers

8. The Security Officer (SO) is responsible for administering the necessary administrative action to ensure compliance with the DSPF on behalf of their Commander, Manager or Defence Industry Security Program member executive. Administrative actions include:

a. recording the details of forms AA 062 Overseas Visit Authority (for official travel) or AB644 – Notification of Proposed Overseas Travel (for private travel) in the Security Register and filing the form at unit level;

b. assisting Defence personnel, Contractors, Consultants and Outsourced Service Providers in complying with their responsibilities as outlined in the DSPF, including assisting those with compartmented briefings to report their private overseas travel to the relevant compartment controller via ASD Security or Communications Intelligence Security Officer (COMSO);

c. providing overseas travel briefings and debriefings, including following up as required anything noted in the completed form AB645 – Overseas Travel Debriefing Certificate (for private travel); and

d. confirming that (if required) an XP090 has been completed and sent to the DS&VS IVO within a suitable timeframe.

9. In the absence of an SO, the Commander or Manager is to organise an appropriate person to provide overseas briefings and debriefings.

Example: *If an individual with a Negative Vetting 1 clearance, and no Sensitive Compartment Information briefs, is working in an area where the unit SO is unavailable to provide a travel brief, the unit COMSO is able to provide the individual with the travel brief/debrief as a last resort.*

Key Definitions

Further Definitions

10. Further definitions for common PSPF terms can be found in the Glossary.

11. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy

Annexes

Annex A – *Overseas Travel Briefing and Debriefing Guide*

Annex B – *Travelling with Portable Electronic Devices and Media*

Document Administration

Identification

DSPF Control	Overseas Travel
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)
DSPF Number	Control 44.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Overseas Travel
Related DSPF Control(s)	Classification and Protection of Official Information Foreign Release of Official Information Contact Reporting Physical Transfer of Information and Assets 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 SPS	Launch

Defence Security Principles Framework (DSPF)

Annex A to Overseas Travel – Overseas Travel Briefing and Debriefing Guides

Briefings

1. Table 1 outlines the process for briefing a traveller prior to their overseas travel.

Note: *The AA062 - International Travel Approval form is currently under development and will be available soon. For all official travel, please use the AB644 - Notification of Proposed Overseas Travel form*

Table 1 – Briefing Process Prior to Overseas Travel

Stage	Who does it	Description
1	Person travelling	For personal travel completes the form AB644 – Notification of Proposed Overseas Travel or for official travel completes the AA 062 – Overseas Visit Authority, and sends it to their Security Officer as soon as they plan to travel. Contacts the relevant agency Security Officer for specific compartmented briefings (if applicable).
2	Security Officer	Provides traveller with copies of the following from the Defence Security Portal: • the Defensive Briefing Before Overseas Travel; and • the Certification of Security Advice Given for Overseas Travel. Conducts an overseas travel briefing with the person travelling. Confirms the person travelling has had any required compartment briefings.
3	Person travelling	Acknowledges, signs and returns the Certification of Security Advice Given for Overseas Travel to the Security Officer. Obtains travel advice for the country(ies) being visited or transited through from the Department of Foreign Affairs and Trade (DFAT) Smartraveller website.

Stage	Who does it	Description
4	Security Officer	Records the travel details in the Security Register. Retains the completed form AB644 (for private travel) or AA062 (for official travel) and signed Certification of Security Advice Given for Overseas Travel at unit/facility level. Conducts a more detailed briefing if: 1) the person travelling has a high level of access; 2) DFAT has issued a Consular Travel Advisory Notice or Bulletin for any country being visited or transited through; or 3) the person is travelling with a Defence or Defence Industry Security Program laptop or Portable Electronic Device (PED) (also referred to as a Mobility Device), and is not protected by a *Laissez-Passer* (refer Definitions below.) If there are any security concerns the Security Officer is to send the completed form AB644 (private) or AA062 (official) to the relevant Defence Security and Vetting Service (DS&VS) regional office.

Debriefings

2. The table below outlines the process for debriefing a traveller returning from overseas.

Table 2 – Debriefing Process When Returning from Overseas

Stage	Who does it	Description
1	Person travelling	Completes the debriefing section of the AB644 (private) or form AB645 - Overseas Travel – Debriefing Certificate (official) and sends it to their Security Officer.
2	Security Officer	Conducts an initial debriefing using the debriefing notes.
3	Person travelling	Completes any of the following forms which are relevant, detailing any suspicious or unusual contact with foreign nationals: • XP168 - Report of Contact of Security Concern; or • XP188 - Security Incident Report.
4	Security Officer	Retains the completed form AB645 at Unit/Facility level. Sends to the DS&VS regional office any completed: • XP168 - Report of Contact of Security Concern; or • XP188 - Security Incident Report.
5	DS&VS Regional Office	If relevant, provides the DS&VS Assistant Director Counterintelligence with information about any security incidents of concern.

Issues Covered in Debriefings

3. Travel debriefing if a formal requirement to discuss events that occurred during the visit, and identify any events which could later be used to threaten the security of the individual. This is a discussion not an interrogation, and therefore the returning traveller should not be questioned as such.

4. Issues covered in the debriefing are outlined below:

5. Travel procedures:

a. **Visa** - How and by whom was the visa obtained? Were any probing questions asked regarding employment?

b. **Entry and exit procedures** - What occurred? Were documents examined out of sight? Were any searches conducted by officers/officials? Were there any troubling interactions with officers/officials? and

c. **Travel arrangements** - Was travel undertaken alone or with an organised party? Was there contact with officials or tour guides in the country and, if so, was there anything about their behaviour to indicate they may have had an intelligence function? Was any special attention paid to the person travelling or to other members of the organised party?

6. Accommodation:

a. Where did the person travelling stay?

b. How and by whom was the accommodation arranged?

c. Was there a choice in accommodation?

d. Did any staff appear to behave in an unusual manner? and

e. Was there any evidence of eavesdropping or searches of luggage or rooms?

(1) Was the person travelling carrying official information while on official travel?

(2) Was this official information appropriately stored and/ or accompanied?

(3) Was this official information left unattended in the traveller's room at any time during the stay? and

(4) Was the traveller's room cleaned or serviced while the traveller was absent?

7. Contact with local nationals:

a. Was any approach made to the person travelling for any of the following reasons:

(1) currency exchange;

(2) bartering, such as an offer to purchase or swap any of the person's belongings;

(3) sexual soliciting; or

(4) requests to carry mail/packages?

b. Was any excessive interest taken in the employment of the person travelling?

c. Was there any unusual contact with any uniformed official?

d. Did anybody propose continuing contact after the visit? and

e. Were any invitations of any type offered?

Note: *This is not a definitive list of questions to ask, or reasons local nationals may seek to make contact with travelling Defence personnel, Contractors, Consultants or outsourced Service Providers.*

8. Contact with other travellers or non-locals living in the country:

a. Did the traveller have any contact with tourists who did not seem to be genuine (e.g. people in their tour group, other guests at their hotel, other visitors to attractions, etc.)?

Definitions

9. ***Laissez-Passer*** - A document issued by a national government or international treaty organisation to allow a government employee to act as a temporary diplomatic courier. The Laissez-Passer confers diplomatic immunity on the contents of a diplomatic pouch carried by the person to whom the Laissez-Passer is issued. However, it does not confer diplomatic immunity on their hand luggage or other belongings. The Laissez-Passer and diplomatic pouch are issued to an individual and are not transferable.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Overseas Travel Briefing and Debriefing Guides
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Overseas Travel
DSPF Number	Control 44.1

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 SPS	Launch

Defence Security Principles Framework (DSPF)

Annex B to Overseas Travel – Travelling with Portable Electronic Devices and Media

Travelling Overseas with a 'Handle As' Classification of UNCLASSIFIED

1. When Defence personnel, Contractors, Consultants and Outsourced Service Providers travel overseas on Defence business with a Defence laptop or Portable Electronic Device (PED), including removable media with an actual classification of UNCLASSIFIED, 'For Official Use Only' (FOUO) or PROTECTED, the Defence laptop or PED is to be encrypted with an Australian Signals Directorate (ASD)-approved product accredited to reduce the 'handle as' classification to UNCLASSIFIED.

2. In these instances approval for carriage overseas is to be sought from, and recorded by, the relevant Security Officer and is to only be given when the travel is for official Defence business purposes. Official Defence business purposes may include private travel if the individual has a confirmed condition of employment to be on call whilst away on private travel. These Defence laptops or PEDs are to be carried as hand luggage.

Travelling Overseas with an 'Actual' Classification of CONFIDENTIAL and Above

3. Defence laptops or PEDs including removable media with a classification of CONFIDENTIAL or above are to be transported utilising either Diplomatic Safe Hand or carried as hand luggage by the Defence member with a *Laissez-Passer* (see Definition below); refer to DSPF Principle 71 – *Physical Transfer of Information and Assets* for further guidance. This applies even if the Defence laptop or PED is encrypted with an ASD approved product to reduce its 'handle as' classification to FOUO.

Storage Overseas

4. Physical access to a Defence laptop or PED may allow covert modification of the device to circumvent the cryptographic controls through techniques such as the installation of a hardware key logger. Defence personnel Contractors, Consultants and Outsourced Service Providers travelling overseas with a Defence laptop or PED are reminded that they are not to store classified or sensitive material in hotel rooms or hotel safes unless that material, including the Defence laptop or PED is stored in a

tamper evident manner, refer to DSPF Principle 71 – *Physical Transfer of Information and Assets* for further guidance.

Requests to Search a Defence Laptop or PED

5. Most countries equate the random search of a laptop or PED with a random luggage search. Defence personnel, Contractors, Consultants and Outsourced Service Providers are not exempt from such searches. They are to comply with the request for a search unless they are carrying a *Laissez-Passer* protecting the Defence laptop or PED.

Key Definitions

6. ***Laissez-Passer***: A document issued by a national government or international treaty organisation to allow a government employee to act as a temporary diplomatic courier. The Laissez-Passer confers diplomatic immunity on the contents of a diplomatic pouch carried by the person to whom the Laissez-Passer is issued. However, it does not confer diplomatic immunity on their hand luggage or other belongings. The Laissez-Passer and diplomatic pouch are issued to an individual and are not transferable.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Travelling with Portable Electronic Devices and Media
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Overseas Travel
DSPF Number	Control 44.1

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 SPS	Launch

Defence Security Principles Framework (DSPF)

Contact Reporting

General principle

1. All Defence personnel, Contractors, Consultants and Outsourced Service Providers should report contacts of security concern to assist in the identification of any attempts to cultivate Defence's people and/or acquire access to official, classified or sensitive materials.

2. All clearance holders are required to report defined contacts with foreign officials or other foreign nationals or any requests from foreign officials to access government assets or security classified information or resources.

Rationale

3. Foreign intelligence services and other threat actors devote considerable resources to obtain access to political, economic, scientific, technological, military and other information. This is not limited to classified information and often includes privileged information. Any compromise may be prejudicial to Australia's National Interest. Small pieces of information could contribute to an intelligence collection process. Accordingly, Defence personnel, Contractors, Consultants and Outsourced Service Providers need to recognise that an 'innocent' conversation or 'contact' (e.g. e-mail, social media) can be part of human intelligence gathering.

4. The Australian Government Contact Reporting Scheme is managed by the Australian Security Intelligence Organisation (ASIO). The Scheme assists ASIO to identify activity directed against Australia and its interests including people who hold an Australian Government security clearance. ASIO uses this intelligence to assist in the formulation of threat assessment and security intelligence advice and to protect the national interest.

Expected outcomes

5. Defence Security and Vetting Service collects and assesses contact reports and coordinates the Defence input into the Australian Government Contact Reporting Scheme;

6. Defence personnel, Contractors, Consultants and Outsourced Service Providers report suspicious, on-going, unusual or persistent contacts with foreign

officials and other foreign nationals (see Implementation Notes, Resources and Tools below);.

7. Defence personnel, Contractors, Consultants and Outsourced Service Providers report instances when an individual or group, regardless of nationality, seeks to obtain official information they do not require access to;

8. Defence personnel, Contractors, Consultants and Outsourced Service Providers understand security threats to inform their reporting obligations; and

9. Security clearance holders understand their obligations under this principle and their responsibilities to report contact which causes security concern (See 'Read in Conjunction With' section below and DSPF Principle 40 – *Personnel Security Clearance*).

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Security Officer, Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	Service or Group Security Authority or Director Security Intelligence and Threats
High	Assistant Secretary Security Threat and Assurance (ASSTA)
Extreme	Defence Security Committee – through ASSTA

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Contact Reporting
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	45
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	N/A
Control Owner	ASSTA

Related information

Government Compliance	**PSPF Core Requirements:** Entity physical security. **Legislation:** *ASIO Act 1979* **Standards:** Joint Directive 32/2014 – Association with Unlawful or Inappropriate Groups by Defence Personnel
Read in conjunction with	Australian Government Contact Reporting Guidelines, September 2010 PSPF – Personnel Security – Reporting Change of Circumstances
See also DSPF Principle(s)	Personnel Security Clearance Identity Security Overseas Travel Counterintelligence Off-site Work Physical Transfer of Official Information, Security Protected and Classified Assets Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Government Contract Reporting Guidelines, September 2010 DS&VS Security Portal Defence Form XP168 - Report of Security Contact Concern [available through DS&VS Security Portal, Defence Industry Portal and through USO]

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

Defence Security Principles Framework (DSPF)

Counterintelligence

General principle

1. Counterintelligence (CI) activities identify and counteract the security risks posed by organisations or individuals engaged in espionage, sabotage, politically motivated violence (including terrorism), criminal activities or other threats to Defence. Defence undertakes CI activities with other intelligence, security and law enforcement agencies that are governed by legislation allowing CI investigations and operations.

Rationale

2. Defence personnel, Contractors, Consultants and Outsourced Service Providers have access to and knowledge of information that could compromise national security through accidental or deliberate disclosure. Defence CI informs the security standards mandated by Government and support the mitigation of risks arising from foreign intelligence services, politically motivated groups, terrorists and disgruntled staff. A robust CI capability will ensure Defence can identify and coordinate a response to threats to Defence.

3. Because of the nature of CI threats, notably from foreign intelligence services, and the sensitive compartmented measures needed to counter these threats, dedicated CI processes and capabilities are required.

Expected outcomes

4. All Groups and Services understand the threat to their people, information, assets and infrastructure and have measures to mitigate them. Where specific process or additional measures are identified to counter specific threats, advice may be provided by DS&VS.

5. Defence personnel, Contractors, Consultants and Outsourced Service Providers have access to timely and relevant security advice.

6. Defence personnel, Contractors, Consultants and Outsourced Service Providers report suspicious, on-going, unusual or persistent contacts with external parties through an XP168 Contact Report (see Implementation Notes, Resources and Tools below.)

7. DS&VS collects, assesses and investigates Contact Reports and, wherever necessary, forwards them to the Australian Security Intelligence Organisation and enacts suitable countermeasures.

8. DS&VS liaises and coordinates with other government agencies for non-operational CI related activities to contribute to a whole-of-government security regime.

9. Joint Operations Command is responsible for coordinating operational CI activities.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Security Officer, Supervisor, Commander or Manager
Moderate	Service or Group Security Authority or Director Security Intelligence and Threats
Significant	Assistant Secretary Security Threat and Assurance (ASSTA)
High	Defence Security Committee – through ASSTA
Extreme	Secretary and Chief of Defence Force

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Counterintelligence
Principle Owner	First Assistant Secretary Security and Vetting Services (FAS S&VS)
DSPF Number	46
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	N/A
Control Owner	ASSTA

Related information

Government Compliance	**PSPF Core Requirements:** Entity physical resources. **Legislation:** *Intelligence Services Act 2001*, *Australian Federal Police 1979 (AFP) Act (Cth)*, *Crimes Act 1914 (Cth)* *ASIO Act 1979*
Read in conjunction with	ADDP 2.1 Counterintelligence and Security
See also DSPF Principle(s)	Classification and Protection of Official Information Personnel Security Clearance Security Awareness and Training Contact Reporting Physical Transfer of Official Information, Security Protected and Classified Assets Security Incidents and Investigations
Implementation Notes, Resources and Tools	ADDP 2.1 Counterintelligence and Security DS&VS Security Portal Defence Form XP168 - Report of Security Contact Concern [via DS&VS Security Portal] *ASIO Act 1979*

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

Defence Security Principles Framework (DSPF)

Working Offsite

General principle

1. Security measures are in place, and practices are followed, to protect official information and assets from unauthorised access when the person using the information or assets is working away from their usual workplace.

Rationale

2. Defence personnel, Contractors, Consultants and Outsourced Service Providers may need to undertake duties outside their usual workplace.

3. When work is being performed outside the usual workplace, there is an increased risk of official information being accessed without authorisation – this may compromise national security, impact Defence capability, or have a negative effect on Defence's reputation.

Expected outcomes

4. Defence personnel, Contractors, Consultants and Outsourced Service Providers protect official information taken outside their usual workplace.

5. Offsite workplaces are properly assessed to identify any security vulnerabilities that need to be addressed before official information is used or stored there.

6. Defence personnel, Contractors, Consultants and Outsourced Service Providers follow security measures and practices to prevent unauthorised access by, or disclosure to, those who do not have the appropriate security clearance and a need-to-know.

7. Defence personnel, Contractors, Consultants and Outsourced Service Providers are aware of the increased security risks associated with working off-site.

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	Band 1/O-7/1 Star (or higher) in Group or Service
High	Assistant Secretary Security Policy and Services (AS SPS)
Extreme	Defence Security Committee (DSC) – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Working Offsite
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	70
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 70.1
Control Owner	AS SPS

Related information

Government Compliance	**PSPF Core Requirements:** Robust information communication technology systems; Access to information; Entity physical resources; and Entity facilities. **Legislation:** *Work Health and Safety Act 2011* WHS Regulations WHS Code of Practice **Standards:** AS ISO/IEC 27001:2015 Information technology – Security techniques – Information security management systems – Requirements
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Audio-visual Security ICT Certification and Accreditation Personnel Security Clearance Contact Reporting Physical Transfer of Information and Assets Physical Security Certification and Accreditation Security Incidents and Investigations

Implementation Notes, Resources and Tools	1. Australian Government, Working away from the office guidelines 2. Australian Government information security management guidelines - Protectively marking and handling sensitive and security classified information 3. Australian Government protective security governance guidelines – Reporting incidents and conducting security investigations 4. Better Practice Checklist – 21. ICT Support for Telework 5. Australian Government physical security management guidelines – Event security 6. Defence People Group Telework Policy 7. Information Security Manual (Working Off-site)

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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Working Offsite

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this enterprise-wide control.

Escalation Thresholds

2. The AS SPS 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 or Service
Significant	Band 1/O-7/1 Star (or higher) in Group or Service
High	AS SPS
Extreme	Defence Security Committee (DSC) – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Introduction

3. When Defence personnel, Contractors, Consultants and Outsourced Service Providers are undertaking approved offsite work within Australia, they are to apply appropriate security controls in accordance with the DSPF and any applicable, referenced material.

4. This policy covers the security of official information and assets. It does not extend to Work Health and Safety (WH&S) matters.

Offsite Work

5. Offsite work includes work undertaken:

a. at the person's Home (whether or not there is an approved Telework arrangement in place);

b. during official travel (for example in a hotel, on an aircraft, or in a conference environment); or

c. at a Defence contractor's premises.

Example: *Mary reviews and drafts official documents and checks her Defence email whilst at her home; she does this on her own computer by logging into Defence Remote Electronic Access and Mobility Services (DREAMS) – which is an accredited gateway.*

6. Prior to approving offsite work arrangements, the approving authority should take into account whether the location being used has been assessed for security vulnerabilities, and the extent to which those vulnerabilities may be mitigated. Refer to 'Approvals' (below) in this Control.

7. In addition to meeting security requirements, Defence personnel may require approval to undertake offsite work in accordance with the Defence Telework Policy.

Protecting Official Information

8. Defence personnel, Contractors, Consultants and Outsourced Service Providers are to ensure that official information is protected from unauthorised access. Refer to DSPF Principle 10 - *Classification and Protection of Official Information*.

9. Defence personnel, Contractors, Consultants and Outsourced Service Providers **must not** allow people without the appropriate clearance, and a legitimate need-to-know, to access official information not authorised for public release.

10. Unless authorised for public release, official information should not be accessed, read or discussed in any setting where people without the appropriate clearance, and a legitimate need-to-know, might hear, record or interact with that information.

11. Where it is reasonable to assume uncleared people cannot see, hear or record the information, approval is not required before accessing the following official information offsite:

a. Information that is UNCLASSIFIED – in either hard copy or electronic (soft copy) format; and

b. Information classified as PROTECTED – in soft copy only, via an accredited remote access system such as DREAMS, or via a device that has a 'handle-as' classification of For Official Use Only (FOUO) or lower. Refer to Key Definitions (below) for an explanation of handle-as classifications.

Example: *Robin is travelling and working from his hotel room on a Defence laptop. He may access official information classified as PROTECTED when using DREAMS to access the Defence network provided that uncleared people cannot see the information..*

12. An auditable record of protectively marked documents and material removed from Defence premises is to be maintained. Material classified SECRET and above **must** be recorded in an XC-40 Classified Document Register (CDR).

13. Security classified information **must** be stored in accordance with the requirements in DSPF Principle 10 - *Classification and Protection of Official Information* and DSPF Principle 72 - *Physical Security*.

Hard Copy Documents

14. Approval is required before Defence personnel, Contractors, Consultants and Outsourced Service Providers may remove PROTECTED and above material from Defence premises to conduct offsite work. Refer to DSPF Principle 71.1 - *Physical Transfer of Information and Assets* and DSPF Principle 72 - *Physical Security* for policy related to the authorised removal of this material - secure storage for the material is required.

15. Information in hard copy (or on a device's screen) with a classification of PROTECTED or above **must not** be accessed or viewed in any setting where the information may be exposed to people without the appropriate clearance, and a legitimate need-to-know. The information is to remain secured in accordance with the DSPF Principle 71 - *Physical Transfer of Information and Assets* at all times in such locations.

Example: *It is a security breach to review hard copy PROTECTED documents whilst sitting in a café, a restaurant, on board a flight, etc.*

Classified ICT Equipment and Media

16. Approval is required before Defence personnel, Contractors, Consultants and Outsourced Service Providers may remove ICT equipment, or media with a 'handle as' classification of PROTECTED or above from Defence premises to conduct offsite work.

17. Encrypted ICT equipment or media with a 'handle as' classification may resume its actual classification once powered up, or when hibernating. Regard **must** be had to where such equipment or media is used in order to ensure that information is not compromised. Refer to 'Actual and 'handle-as' security classifications for

encrypted devices and media' in Key Definitions below and to any SOPs for the specific equipment.

Example: *A Defence laptop with an actual classification of PROTECTED has its handle-as classification reduced to UNCLASSIFIED by ASD-approved encryption. The laptop is put into hibernation mode at work and taken home prior to an offsite meeting the next day – this leaves the laptop unencrypted and its security must therefore be managed in accordance with its actual classification of PROTECTED.*

Classified Conversations

18. Conversations involving classified information should not occur where persons without the appropriate clearance, and a legitimate need-to-know, may overhear or utilise other technological means to eavesdrop on or record the conversation.

Example: *Although secure mobile phones with ASD-approved encryption allow the user to make classified calls from unsecured areas, this introduces the risk of eavesdropping on the people having the conversation.*

19. Offsite classified conversations are to be protected from being overheard or recorded. See PSPF Physical Security Management Guidelines – Working away from the office for guidance on the measures that can be used to reduce the threat of conversations being overheard or recorded.

20. Where classified conversations are conducted at home, e.g. on a secure phone, attention needs to be paid to the presence of uncleared persons.

Example: *Children over the age of ten years generally have a well-developed long term memory, a good ability to comprehend information, and a strong sense of curiosity. Exposing them to classified information is a security risk.*

21. Where there is an expectation that classified discussions will occur regularly at home, advice on audio security countermeasures **must** be sought from the Defence Security and Vetting Service (DS&VS).

Note: *There is an increased risk of Foreign Intelligence Services (FIS) targeting premises where classified conversations occur regularly.*

Overnight Carriage

22. Overnight carriage of classified information is covered in DSPF Principle 71 - *Physical Transfer Information and Assets*. Relevant material is to remain secured in a tamper-evident enclosure whilst in transit between secure locations, appropriate locations for overnight stops, or locations approved for offsite work.

Geo-location Security

23. Geo-location is the process or technique of identifying the geographical location of a person or device by means of digital information processed via the Internet.

24. In the rare event the location of an out of office trip is classified, location data is to be protected by:

a. not using a mobile telephone (ID/SIMM cards could be used to track the device);

b. turning off any GPS equipment or applications;

c. disabling any application location services;

d. not logging into any social networks; and

e. not taking photos.

Note: *Geo-location security may apply to operations and operational areas, requiring that their location remains unknown to those without both a need-to-know and a right-to-know. Further details will be covered in any Operational Security instructions.*

Physical Storage Requirements for Offsite Work

25. Defence personnel, Contractors, Consultants and Outsourced Service Providers conducting offsite work are required to comply with procedures for handling and protecting official information during its use, storage, transfer and transmission. Refer to DSPF Principle 72 - *Physical Security* and DSPF Principle 71 - *Physical Transfer of Information and Assets*.

26. Whilst undertaking offsite work, ICT equipment and media is to be stored in accordance with the Information Security Manual (ISM) – ICT Equipment and Media chapter.

27. Accredited remote access systems, and products that implement ASD-approved encryption, may have the effect of reducing the actual classification of material to a lower 'handle-as' classification when the encryption is active.

Note: *These protection measures will not work unless the encryption is activated. A device in standby power mode may not be protected, so users are to follow the device's Standard Operating Procedures (SOPs) and ensure it is in a secure state when left unattended.*

Example: *A Defence laptop is being used to process and store information up to the classification of SECRET and as such the laptop itself has a classification of SECRET. ASD approved encryption is*

used to reduce the device's 'handle-as' classification to UNCLASSIFIED. A security container is not, therefore, required to store the device when it is powered off – although the device still requires normal protections from fire and theft. When the device is powered on or in hibernation mode then it resumes its classification of SECRET and should be stored accordingly.

28. If information or assets with a 'handle-as' classification of PROTECTED or above need to be stored at Home, authorisation for offsite work is required.

Disposal of Official Information

29. Defence personnel, Contractors, Consultants and Outsourced Service Providers working offsite are required to dispose of classified waste in accordance with DSPF Principle 10 - *Classification and Protection of Official Information*. If classified waste cannot be disposed of appropriately when offsite, it is to be securely stored until it can be securely transferred to a facility where proper disposal may occur.

Reporting Security Incidents

30. When Defence personnel, Contractors, Consultants and Outsourced Service Providers working offsite become aware of any incident that may indicate or suggest that security classified or official material has been compromised, tampered with or stolen, they are to immediately report this in accordance with the DSPF Principle 77 - *Security Incidents and Investigations*.

31. Any recommended remedial action arising from an incident **must** then be taken by the employee.

Example: *A failed break and enter at a home-based work property may require investigation or additional security measures to be implemented even though there is no evidence of Defence material being targeted.*

Approvals

Remote Access Approvals

32. Defence permits remote access to some of its ICT networks via accredited remote access solutions (e.g. DREAMS). Policy pertaining to the use of remote access is located in DSPF Principle 30 - *Remote Access to Defence Systems*.

33. Remote access up to CONFIDENTIAL and SECRET information and networks, excluding CODEWORD systems, requires the approval of the user's Commander or Manager.

34. Remote access to TOP SECRET and CODEWORD information and networks requires the approval of the Deputy Secretary Strategic Policy and Intelligence (DEPSEC SPI).

35. It is not permitted to reclassify information to allow it to be sent, or accessed from, offsite. Reclassifications are only to occur in line with DSPF Principle 10 – *Classification and Protection of Official Information*.

Example: *Bob reclassifies a SECRET document to PROTECTED in order to be able to access it remotely from home. This is a security breach and is not allowed.*

Offsite Work Approvals - Physical

36. Offsite work requiring the physical handling, storage or destruction of material with a 'handle-as' classification of PROTECTED or above, other than CODEWORD information, requires the approval of (at minimum) an SES Band 1/O7 in the user's chain of command or the First Assistant Secretary Security and Vetting Services (FAS S&VS). This role may not be delegated.

37. Additional approval may be required from the originating agency when Defence is not the sole originator of the classified material.

38. Offsite work requiring the physical handling, storage or destruction of material classified TOP SECRET, or that carries a CODEWORD, requires the approval of DEPSEC SPI. This authority may not be delegated below SES Band 1/O7, and additionally requires the prior approval of both ASIO and the originating agency.

39. The following questions are to be considered when approval for offsite work is being considered:

a. Current Security Risk Assessment (SRA);

b. Is there a real need to remove the classified material from Defence premises?

c. Are there appropriate storage options at the offsite work site for the classified material being stored, handled or destroyed? This will require the approval authority to strike a balance between the requirements for offsite work with the physical security measures in place at the location;

d. Have the ICT systems to be used been accredited to handle the highest classification of work to be conducted in accordance with DSPF Principle 73 - *Physical Security Certification and Accreditation*;

e. Have SOPs for the transfer, handling, storage and destruction of official information at the home-based site been developed?; and

f. Has the employee been briefed by their Security Officer on the policies contained in the PSPF, this DSPF part and any agreed SOPs?

40. Material is to remain in the personal custody of the individual and stored appropriately when not in use, in accordance with PSPF Core Requirements and DSPF Principle 72 - *Physical Security*.

Standard Operating Procedures

41. In addition to a formal agreement to undertake offsite work, it may be appropriate to develop SOPs – these may include:

a. specifying the maximum classification of work to be conducted by the employee off site including:

   i. classification of discussions allowed;

   ii. classification of information processed on ICT systems; and

   iii. classification of information stored, handled or destroyed;

b. the requirement for a completed and current (no more than 24 months old) SRA covering the place where offsite work will occur;

Example: *The security assessment should address security matters (including physical security) - additional assessments may be required from a Work Health and Safety perspective.*

c. identifying the equipment that is to be supplied by either party or shared in order to perform the duties;

d. any restrictions on equipment usage;

Example: *Susie has carer responsibilities and has been provided a Defence laptop to be able to work from home. It is not permissible for her child to use the laptop to browse the internet even while supervised by Susie.*

e. whether ICT or physical certification and accreditation is required and where copies of the relevant certificate(s) will be held;

f. whether Defence has the right to conduct compliance checks and determine how official resources are protected at the home-based site;

g. procedures for the secure handling, storage and destruction of official information, including the provision of security containers suitable to store the maximum classification of information to be held;

h. procedures for the disposal or return of classified waste;

i. the requirements to report any security incidents at the premises to DS&VS; and

j. procedures for the transfer of classified material between other Defence or approved premises and the home-based site;

k. confirming the holder is prepared to accept responsibility for the safe custody of any material accessed while offsite.

Accreditation

42. For accreditation purposes, a home-based site is considered the same as any other Defence facility. Refer to the DSPF Principle 73 - *Physical Security Certification and Accreditation* to determine if accreditation is required.

43. Physical accreditation of a home-based site is not required where:

a. official information is only accessed in electronic form, the information's classification is PROTECTED or below, and the offsite device used to access the information is protected by an ASD-approved encryption that reduces the 'handle-as' classification to UNCLASSIFIED or FOUO when the device is not in use;

b. hard copies of information handled, stored or destroyed do not exceed the security classification of UNCLASSIFIED.

Compliance Checks

44. Regular compliance checks relating to the security requirements for offsite work may be conducted in accordance with the terms and conditions outlined within the Defence People Group Flexible Working Arrangements.

Example: *Repeated security lapses during unsupervised periods may indicate a need to discontinue offsite work arrangements.*

Protecting Official Information at Events such as Conferences and Workshops

45. Official information, compromised in any environment, has the potential to undermine Defence's reputation. Consideration should be given to the risks associated with having official information or material at any event, activity or meeting.

46. Security instructions should be developed before any event is held in a public venue or Zone One area involving classified information, classified assets or other official information that has not been approved for public release.

47. Security instructions can be simple but need to be tailored to the event and based on a current SRA. Depending of the nature of the event, they should consider items including:

a. entry and access control, including identification of staff and visitors, escort requirements, ratio of visitors to escorts;

b. the carriage/transfer of official information to and from the venue;

c. security clearances of facilitators, venue staff and escorts who may have access to classified material;

d. the storage and handling of official information that is not for public release, including disposal and reproduction;

Example: *Kylie uses the photocopier at a conference venue to copy official information that she needs to use for her presentation – this may leave a copy of the document in the machine's memory that could later be accessed by unauthorised people.*

e. access control procedures;

f. reporting process and requirements for security incidents;

g. security of equipment on display or in attendance;

h. the possibility of protest action or Foreign Intelligence Service collection activity (advice on these matters may be sought from DS&VS); and

48. In the case of CODEWORD material, the agreement of the relevant compartment controller must be gained prior to the material being taken to any offsite event.

49. If classified information is to be discussed in non-accredited areas, advice **must** be obtained from either DS&VS, or in the case of CODEWORD information, compartment controllers. Technical Surveillance Counter Measures (TSCM) may also be required. Refer to DSPF Principle 14 - *Audio-visual Security*.) TSCM advice should also be obtained following any such discussions.

50. If classified information or assets need to be stored in a Zone One or Two event site, for example overnight storage, advice should be obtained from the DS&VS regional office. Refer to DSPF Principle 72 - *Physical Security*).

51. For more general guidance on event security refer to the PSPF Physical Security Management Guidelines: Event Security.

Roles and Responsibilities

Deputy Secretary Strategic Policy and Intelligence (DEPSEC SPI)

52. DEPSEC SPI is responsible for approving:

a. offsite work involving the handling, storage or disposal of information that is classified TOP SECRET or carries a CODEWORD; and

b. remote access to TOP SECRET and CODEWORD information and networks.

CODEWORD Compartment Controllers

53. Compartment controllers are responsible for providing advice to DEPSEC SPI with regard to the approval, or otherwise, of offsite work involving official information that carries any CODEWORD for which they have a compartment control responsibility.

54. For compartments managed on behalf of external agencies, compartment controllers are to liaise with those agencies on matters of shared security risk.

First Assistant Secretary Security and Vetting Service (FAS S&VS)

55. FAS S&VS is responsible for ensuring the assessment of security arrangements for, and managing any accreditation of, home-based work environments for Defence personnel, Contractors, Consultants and Outsourced Service Providers employed in joint service, Defence civilian units and DISP facilities.

Executive Security Advisers (ESA)

56. Executive Security Advisers (ESA) are responsible for assessing the security arrangements for, and managing any accreditation of, home-based work arrangements for Defence personnel, Contractors, Consultants and Outsourced Service Providers employed in single-service units.

Commanders, Managers and Contract Managers

57. Commanders, Managers and Contract Managers are responsible for the approval of offsite work:

a. where physical storage is required for UNCLASSIFIED information;

Note: *Commanders, Managers and/or Contract Managers cannot approve offsite work that requires physical storage of information with a 'handle-as' classification of PROTECTED or above.*

b. for remote access (such as DREAMS) to systems up to PROTECTED (this does not include hard copy documents).

Note: *In the majority of cases, Defence-supplied accommodation is not suitable for the conduct of classified work.*

Outsourced Service Provider Managers

58. Outsourced Service Provider Managers are to gain the approval for offsite work for any affected staff from or through the relevant Defence Contract Manager before permitting work from home to be conducted using Defence information.

Key Definitions

59. **Home.** A private dwelling, Defence supplied accommodation (including service accommodation in barracks and on exercise), or an approved alternative place of work.

Exclusion: *For industry, where the private dwelling is the primary place of business it is considered as a facility and requires accreditation in accordance with DSPF Principle 73 - Physical Security Certification and Accreditation.*

60. **Offsite Work.** Offsite work is work undertaken in any location not recognised as a usual workplace. This does not include work conducted on operations (with the exception of approval processes for the conduct of classified work in accommodation areas such as barracks) and does not cover Defence ICT support to Australian Defence Force (ADF) deployments.

61. **Home-based Site.** A security accredited private dwelling or other location that has been agreed between Defence and an employee as regular place of work.

62. **Home-based Employee.** An employee working at a home-based site.

63. **Home-based Work Agreement.** A formal agreement between an employee and Defence documenting the conditions of home-based work.

64. **Public Site.** Any place where neither the employee nor Defence can exert physical control over the local environment e.g. hotels, conference rooms, public transport, airport lounges etc.

65. **Defence Controlled Device.** A device is under Defence control if it is owned by Defence or is subject to any agreement that legally binds the owner of the device to comply with all DSPF and ISM security policies. Defence controlled devices include security classified assets owned by Defence Industry Security Program (DISP) members.

Example: *A DISP member supplies their own computer to process SECRET information. DISP membership contractually obliges the company to comply with all Commonwealth policies and the DSPF therefore the device is under Defence control.*

66. **Privately Owned Device.** Is a device where the end user has administrative control, responsibility and legal authority over the device's configuration. End users can exert control over these devices.

Example: *A home computer or personal mobile phone. The end user can install their own virus detection software.*

67. **Public Device.** A subset of Privately Owned Devices where the end user has no administrative control over the device, they are not responsible for, and have no legal authority over, the configuration of the device.

Example: *Internet kiosks and shared computers in hotels.*

68. **Australian Signals Directorate Approved Encryption.** Any cryptographic functionality that is implemented in accordance with all of the relevant requirements of the ISM Cryptography Section (including any product specific advice or in the Australian Communications Security Instructions (ACSI) series publications) in order to reduce the handling and storage requirements of the device.

69. **Actual and 'handle-as' Security Classifications for Encrypted Devices and Media.** Where ASD-approved encryption is applied to a device/media, that device/media has two different classifications. These are:

a. the **actual classification**: the highest classification of information stored on or processed by the device/media, regardless of whether encryption has been applied;

Note: *This classification also applies whenever the device/media is in a keyed state, i.e. where the classified information is accessible in an unencrypted form.*

b. the **'handle-as' classification:** the classification of the device/media when the classified information it contains is fully protected by encryption;

Note: *This classification enables the device to be stored and physically transferred at a reduced classification due to the protection provided to stored information through the application of suitable ASD-approved encryption technology.*

Note: *If ASD-approved encryption is not used, the actual and 'handle-as' classifications are the same, i.e. the highest classification of data stored or processed on the device/media.*

Exclusion: *Some ASD-approved technologies such as remote access solutions (e.g. DREAMS) have been evaluated to ensure that information is not recoverable from the hosting device once the session ends. In these instances the product's evaluation documentation will advise of the levels of protection offered.*

Further Definitions

70. Further definitions for common PSPF terms can be found in the Glossary.

71. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Working Offsite
Control Owner	AS SPS
DSPF Number	Control 70.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Working Offsite
Related DSPF Control(s)	Classification and Protection of Official Information Audio-visual Security ICT Certification and Accreditation Personnel Security Clearance Contact Reporting Physical Transfer of Information and Assets 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 SPS	Launch

Defence Security Principles Framework (DSPF)

Physical Transfer of Information and Assets

General principle

1. Defence is to ensure that official information, and security protected and classified assets, are transferred in a secure manner and are only received by the intended recipient.

Rationale

2. Official information, and security protected and classified assets, are vulnerable to loss or compromise when being transferred, which may have negative impacts on Defence and wider Government.

Expected outcomes

3. Official information, and security protected and classified assets, are:

a. to remain secure and uncompromised during transfer;

b. only transported by authorised people or entities;

c. tracked during their physical transfer; and

d. received by the intended recipient.

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 Security Policy and Services (AS SPS)
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Physical Transfer of Information and Assets
Principle Owner	FAS S&VS
DSPF Number	Principle 71
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 71.1
Control Owner	AS SPS

Related information

Government Compliance	**PSPF Core Requirements** **Other:** Vienna Convention On Diplomatic Relations (1961) Articles 27 and 40
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Communications Security (COMSEC) Information Systems (Logical) Security Overseas Travel Working Offsite Physical Security Security Incidents and Investigations Explosive Ordnance Security Radioactive Sources Escorting Security Protected or Classified Assets

Implementation Notes, Resources and Tools	• Australian Government physical security management protocol • ASIO, Security Equipment Guides (SEGs) are available to ASAs from the GovDex Protective Security Community • Security Equipment Evaluated Product List (SEEPL) – refer also Security Toolkit: Security Equipment Guides • Defence Courier Service (DCS) contract user guide • Australian Radiation Protection and Nuclear Safety Agency Security of Radioactive Sources – Code of Practice

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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Physical Transfer of Information and Assets

Redacted Veriosn: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. Assistant Secretary Security Policy and Services (AS SPS) is the owner of this enterprise-wide control.

Control

2. This section of this DSPF Enterprise-wide Control is For Official Use Only and has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – *Transport of Bulk Assets*

Annex B – *Developing a Movement Security Plan*

Document Administration

Identification

DSPF Control	Physical Transfer of Information and Assets
Control Owner	AS SPS
DSPF Number	Control 71.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Physical Transfer of Information and Assets
Related DSPF Control(s)	Classification and Protection of Official Information Communications Security (COMSEC) Information Systems (Logical) Security Overseas Travel Working Offsite Physical Security Security Incidents and Investigations Explosive Ordnance Security Radioactive Sources Escorting Security Protected or Classified Assets

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 SPS	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex A to Physical Transfer of Information and Assets Transport of Bulk Assets

General Requirements

1. Classified and high-risk unclassified assets are to be transported in accordance with the policy below based on their assigned Business Impact Level (BIL). Both classified and high-risk unclassified assets will have BILs assigned to them. Refer to BIL guidelines within the Protective Security Policy Framework (PSPF).

2. Where an asset has an assigned BIL which is higher than its corresponding classification due to higher integrity/availability factors, the appropriate BIL **must** be used to base transport measures upon. This is because measures based on the BIL will deal more adequately with the risk faced during transport due to the higher level of consequence of loss or damage to the asset.

Example: *A high-risk unclassified asset (Confidentiality BIL of 1 (Low - Medium)) has an assigned BIL of 4 (Extreme) due to the higher level of consequence to Defence if the asset were to be lost (Availability BIL of 4 (Extreme)). As the BIL is higher than the classification, the asset will be more securely transported if the measures were based upon the BIL.*

Packaging

3. Classified and high-risk unclassified assets are to be packaged appropriately so that they are not exposed or damaged during transit. To achieve this, security-protected assets assigned a BIL of 2 (High) and above (classification of PROTECTED and above) are to be packaged and sealed in a manner that ensures:

a. anonymity and security from viewing is achieved;

b. the packaging is tamper evident;

c. the asset is protected against damage;

d. the chance of loss is minimised; and

e. the opportunity for theft is reduced.

Note: *The Supply Chain Branch of Joint Logistics Command can provide advice on appropriate methods of packaging and sealing.*

Movement Security Plan

4. A Movement Security Plan (MSP):

a. **must** be developed for the transport of assets:

(1) assigned a BIL of 4 (Extreme) or 5 (Catastrophic); or

(2) classified SECRET or TOP SECRET;

b. should be developed for the transport of assets:

(1) being transferred internationally;

(2) assigned a BIL of 2 (High) or 3 (Very High); or

(3) classified PROTECTED or CONFIDENTIAL.

c. is recommended for unclassified assets assigned a BIL of 1 (Low-Medium). For guidance on how to develop an MSP, refer to Annex B of this Control.

Guarding and Escorts

5. The question of whether guards or escorts are required is to be addressed in the MSP. For further information regarding escorting, refer to the DSPF Principle 81 – *Escorting Security Protected or Classified Assets*.

Despatching and Receipting

6. Despatching and receipting of security-protected assets is to be in accordance with requirements within the Electronic Supply Chain Manual. For assets assigned a BIL of 2 (High) and above (classification of PROTECTED and above), a signature (including the signatory's printed name and date of signature) is to be obtained on despatch and receipt. At every point where such assets are transferred, a receipt is to be provided by the gaining entity. Whatever receipting method is used, both issuing and gaining entities are to adhere to any applicable 'follow-on' actions described in the receipt.

Airport Screening

7. Assets being transported by air are generally screened for drugs, explosives and other prohibited and dangerous items. Some issuing entities may seek an exemption from screening due to the effect of screening on the nature of the asset. Issuing entities are to seek DS&VS approval for an airport screening exemption if they believe their asset falls into this category.

Transfer of Security Protected Assets by General Freight

8. BIL of 1 (Low - Medium): Security Protected Assets assigned a BIL of 1 (Low - Medium) may be transported by general freight if the requirements of paragraphs 3 and 6 above, have been satisfied.

9. It is recommended that a risk assessment determine whether there is a need for any additional security measures during transfer by general freight, such as but not limited to the use of:

a. locks or security branding; and

b. using SCEC-endorsed couriers instead.

10. BIL of 2 (High) and above: Security Protected Assets assigned a BIL of 2 (High) and above are to meet the following minimum requirements for transfer:

a. by road: Assets are to be transported in a locked vehicle, or a secured container. If transport in a locked vehicle or container is not possible, sheeting or casing sealed with wire and SCEC approved security seals are to be used;

b. by rail: Assets are to be transported in a locked van. Assets with a BIL of 5 (Catastrophic) (classification of TOP SECRET) are to be dispatched in a separate locked and sealed van;

c. by air: Assets are to be sent by either service aircraft or by SCEC endorsed courier. Assets with a BIL of 5 (Catastrophic) (classification TOP SECRET) are to be dispatched by SAFEHAND in either a service aircraft or by SCEC endorsed courier; and

d. by sea: Assets are to be labelled ‘LOCKUP STOWAGE’ and carried in an appropriate locked and secured area/sealed container when transported by RAN or civilian ships.

11. Locking requirements: If the locking up of assets in vehicles or containers has been specified in paragraph 10, it is recommended that:

a. commercial padlocks be used for assets with a BIL of 2 (High) and 3 (Very High); and

b. SCEC-approved padlocks be used for assets with a BIL of 4 (Extreme) and 5 (Catastrophic).

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Transport of Bulk Assets
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control)
DSPF Control	Physical Transfer of Information and Assets
DSPF Number	Control 71.1

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 SPS	Launch

Annex B to Physical Transfer of Information and Assets Developing a Movement Security Plan

Developing a Movement Security Plan (MSP)

1. A MSP is used to document the risks and mitigation strategies involved in the movement of classified information or assets, including weapons or explosive ordnance. All movements are to be planned so they are effected as quickly as possible and the information and assets are protected from unauthorised access. Except for operational movements, planning is to allow six working days' notice for Defence preparation.

Note: *There is no set template or format for a MSP.*

2. A single MSP can be used to cover periodic movement of the consignment between the same parties at fixed departure and destination points. The route, time of departure and halting places are generally varied for each consignment.

Example: *It is not necessary to develop a MSP for each occurrence of a regular movement such as transporting weapons and explosive ordnance to a live-fire range.*

3. The MSP outlines the proposed security measures for the journey. It is recommended that the following details be included in an MSP:

a. name of the issuing entity;

b. name, address and phone contacts of the gaining entity;

c. consignment details, including:

(1) description of the information or assets, including their security classification;

(2) unusual features requiring special handling or storage;

(3) measurements and weights;

(4) supervision of loading and unloading;

(5) method of transmission of equipment keys; and

(6) arrangements for Customs inspection and sealing, if appropriate;

d. movement details, including:

(1) approximate dates;

(2) proposed method including details of the route, en route storage details and name of carrier, as appropriate;

(3) contingency plans (including a detailed response/recovery plan) in the event of a breakdown, accident, diversion or delay;

(4) actions taken or plans for addressing the risks identified in the risk assessment; and

(5) details of security guards or escorts; and

e. A clear outline of the steps to be taken when confronted with an unforeseen circumstance e.g. vehicle breakdown, an attack on the items being transported. This outline should include:

(1) Possible risks including likelihood;

(2) Mitigations including the steps to be taken to address the risks e.g. setting up a piquet to protect weapons or ammunition, Commander to call the police.

4. It is recommended during the drafting of an MSP, that the Defence Security and Vetting Service (DS&VS) be contacted for any threat advice that may affect the security of the freight, especially when SAFEBASE levels have been raised.

5. All MSPs for classified information or assets to be transported overseas are to be submitted to DS&VS for checking against the provisions of any Security of Information Agreements or Arrangements.

6. MSPs are to be approved by the relevant Commander or Manager responsible for the transport of the asset(s). Once approved, issuing entities are to provide a copy of the MSP to the relevant DS&VS regional office or Executive Security Adviser (ESA) for their awareness.

Notice of Movement

7. Once an MSP has been approved, the issuing entity is to prepare and send a Notice of Movement to the gaining entity so that they can prepare to receive the information or assets. The Notice of Movement will generally include the:

a. equipment description and its security classification;

b. security arrangements affecting the gaining entity (which may need to make special arrangement for the security of the equipment after receipt);

c. methods of transportation;

d. date and time of departure of the consignment;

e. location at which the information or assets, and responsibility for it, will be handed over; and

f. estimated date and time of arrival of the consignment.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Developing a Movement Security Plan
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Physical Transfer of Information and Assets
DSPF Number	Control 71.1

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 SPS	Launch

Defence Security Principles Framework (DSPF)

Physical Security

General Principle

1. Defence facilities, people, official information, and security protected assets are protected from unauthorised access, sabotage, wilful damage, theft or disruption through a safe and secure physical environment.

Rationale

2. Application of physical security measures consistent with whole of Government requirements will:

a. ensure a secure physical environment for storage and handling of official resources;

b. facilitate sharing of information and assets across Government, with allies and Contractors, Consultants and Outsourced Service Providers; and

c. maintain a safe and secure working environment for Defence personnel, Contractors, Consultants and Outsourced Service Providers and the public.

Expected Outcomes

3. Appropriate security measures for the protection of resources and people are implemented, and underpinned by a high level of security awareness.

4. Security standards are applied and maintained consistently across the Defence enterprise at a level never lower than whole of Government (Protective Security Policy Framework (PSPF)) requirements.

5. The physical security environment is based on a thorough security risk review incorporating threat and risk assessments.

6. Implemented physical security controls do not breach relevant employer occupational health and safety obligations.

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 Security Policy and Services (AS SPS)
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Note: *Chief of Joint Operations (CJOPS) or an authorised delegate can accept Significant to Extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.*

Document Administration

Identification

DSPF Principle	Physical Security
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 72
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 72.1
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)

Related information

Government Compliance	**PSPF Core Requirements:** Role of accountable authority; Security planning; Security governance for international sharing; Entity physical resources; and Entity facilities.
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Information Systems (Physical) Security Working Offsite Physical Transfer Information and Assets Physical Security Certification and Accreditation Access Control
Implementation Notes, Resources and Tools	Australian Government, Physical security management protocol Australian Government, Security zones and risk mitigation control measures guidelines Australian Government, Business Impact Levels guidelines

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

Defence Security Principles Framework (DSPF)

Physical Security

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this Enterprise-wide Control.

Escalation Thresholds

2. The Assistant Secretary Security Policy and Services has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

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 Security Policy and Services (AS SPS)
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Note: *Chief of Joint Operations (CJOPS) or an authorised delegate can accept significant to extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.*

Controls

General

3. The PSPF sets out minimum physical security controls required for protecting security-protected assets (refer to Key Definitions.) These controls provide a level of assurance that information originators and asset owners need to be confident that the information and assets they share with others will be protected in the same way and to the same level.

4. PSPF policy and guidance is at:

a. Australian Government physical security management protocol;

b. Defence Security Toolkit - ASIO Technical Note 1/15 (Zones 2 - 4);

c. Defence Security Toolkit - ASIO Technical Note 5/12 (Zone 5);

d. Australian Government physical security management guidelines;

e. Security zones and risk mitigation control measures guidelines;

f. Physical security of ICT equipment, systems and facilities guidelines;

g. Working away from the office guidelines; and

h. Business impact levels guidelines.

Information Originators and Asset Owners

5. Originators of information and asset owners and are to determine the appropriate Business Impact Level (BIL) to be applied to the confidentiality, integrity and/or availability for the information or asset. This process is to be in accordance with Business impact levels.

6. Where a BIL is assigned to the confidentiality of official information or an asset, a security classification is to be applied. Refer to DSPF Principle 10 – *Classification and Protection of Official Information*.

Information and Asset Custodians

7. Information and asset custodians are responsible for securing security-protected assets in a manner that is compliant with the PSPF and appropriate for the BIL assigned by the information originator or asset owner.

Determining Physical Security Risk Mitigation Measures

8. Commanders and Managers, who are information and asset custodians, are to determine the most suitable Security Zone for the protection of security protected

assets based on the classification or business impact level of the asset(s) (refer to Identification of Security Zones in this DSPF Control and PSPF - Security zones and risk mitigation control measures.) Additional factors to consider when determining the required level of Security Zone include:

a. specific requirements determined by the information originator / asset owner in accordance with any Defence Instruction or publication specifically related to the information or asset(s);

b. the location of the information or assets within a base or facility;

c. increased threats to Defence, a site or facility;

d. the structure and location of an existing building or site; and

e. additional physical protection systems (e.g. CCTV, access control systems, and alarms).

9. Where Commanders and Managers believe there is a need for physical security controls that exceed the minimum standard, this needs to be substantiated through a formal security risk management plan. This may include the need to store and handle the asset(s) in a higher Security Zone, or to apply stronger individual controls within the same Security Zone.

Note: *It is recommended that information and asset custodians involve other relevant Commanders and Managers during the risk assessment process, such as the Base Support Manager (BSM). It may become apparent during the process that requested physical controls may already have been considered as part of Estate management, not be provided or be inappropriate given other controls already established on the base or facility. Mitigation measures may involve a physical re-location of an asset or unit within a base or facility to a more appropriate Security Zone.*

10. Security Construction and Equipment Committee (SCEC)-approved security containers can be used to provide additional physical security controls. They are designed for storage of classified information/assets. They are not suitable for the storage of high risk unclassified assets. Due to their design these containers provide a high level of tamper evidence of covert attack and significant delay from surreptitious attack, but limited protection from forcible attack. For further information on selecting the appropriate security container refer to Security zones and risk mitigation control measures. For further guidance, refer to Table 1 in Annex A of DSPF Control 72 – *Physical Security*.

11. It is recommended that classified information be stored separately from other security-protected assets. This will:

a. lower the likelihood of compromise of information if assets are stolen; and

b. assist investigators to determine the reason for any incidents involving unauthorised access.

c. Custodians with large quantities of security protected assets may use a Secure Room, strongroom or vault (including SCEC approved Instavaults), instead of containers to protect the information or assets. Secure Rooms are constructed to protect classified information from covert attack. Secure Rooms are constructed as Class A, Class B or Class C Secure Rooms, in accordance with ASIO Technical Notes 7/06, 8/06 and 9/06 respectively.

Note: *Units are to seek advice from the Defence Security & Vetting Service (DS&VS) or the Executive Security Adviser (ESA) of the relevant Service before installing a commercial vault or strong room for the protection of security-protected assets.*

12. Access to security-protected assets is to be based on a legitimate need to know, an appropriate security clearance and sanctioned by a policy, duty statement or directive. Where required, access is to be controlled to Defence bases, facilities, and security-protected assets.

13. Access control can be achieved through a mixture of physical security measures including, but not limited to - building construction techniques, security containers, perimeter, pedestrian and vehicle barriers, access control systems, locks and keying, and guards. All of these things are further defined using the Zone methodology described within the PSPF.

14. For further information on application of access control refer to the DSPF Principles for:

a. *Access Control*;

b. *Classification and Protection of Official Information*; and

c. *Personnel Security Clearance*.

Security Zones

15. Security Zones describe areas on a site that process, handle and store security-protected assets. They are designed to protect security-protected assets of a specific BIL.

16. The primary outcome of the Security Zone methodology is to establish scalable levels of protection from unauthorised or covert access to, and/or forcible attack on security-protected assets, depending on the business needs of the asset owner/custodian.

Identification of Security Zones

17. Facility owners, in consultation with system owners, asset custodians and other relevant stakeholders (such as Senior Australian Defence Force Officers (SADFO) and Heads of Resident Units (HRU), are to identify those areas on a base or within a facility that process, handle and store security-protected assets and

categorise those areas according to the Security Zone methodology described within PSPF guidelines (refer to Security zones and risk mitigation control measures guidelines.)

18. The identification of areas as Security Zones is used for the purposes of base or site planning and differs from the certification and accreditation process. Where required, assistance may be sought from DS&VS or relevant ESA.

19. Once Zones have been identified and categorised, facility owners **must** seek certification and accreditation of those Zones by the appropriate authorities in accordance with DSPF Principle 73 – *Physical Security Certification and Accreditation*.

20. In an area of operations, it is recommended that the relevant Task Force Commander appoint an individual to identify and categorise those areas that process, handle and store security-protected assets.

21. Areas within a site that are not used to process, handle or store security-protected assets are not required to be categorised.

22. Security Zones are to be categorised according to:

a. the level of access to people, information and assets provided by the security controls; and

b. the minimum physical security controls used to treat identified risks in accordance with Security zones and risk mitigation control measures guidelines, Table 3: Zone Requirements.

Example: *The security of a facility is related to its design and level of access control. A facility that is constructed to a Zone Four standard, yet provides unfettered access to the public is not a Zone Four, it remains a Zone One area.*

Portable Electronic Devices Prohibited Zone

23. Portable Electronic Devices (PEDs) are portable devices that can capture, process, store, record or communicate information electronically. Most PEDs are capable of internet connection via Wi-Fi or cellular data, and also contain media, which may be removable or fixed within the device (see ISM section ‘Media Usage’.) Examples of PEDs, official or privately owned, that may be found within Defence include but are not limited to:

a. laptops, tablets, eReaders, mobile phones, cameras, audio players/recorders;

b. data transfer and format converters, that transfer information between peripherals without the use of an intervening computer, such as portable Wi-Fi hotspots, one touch backup drives, Serial Advanced Technology

Attachment (SATA) hard disk to Universal Serial Bus (USB) converters. USB host transfer devices and wireless speakers; and

c. cordless telephones such as Digital Electronic Cordless Telecommunications (DECT) phones, two way radios, and other wireless protocols including WiFi and Bluetooth.

24. Technological convergence has led to most devices incorporating the options of telephony, internet or other data connectivity. Whilst convenient, the security aspects of all functions, including the potential for covert access to microphones, cameras or media within a device will require consideration.

25. TOP SECRET areas **must** be designated as PED-prohibited areas (ISM control 0346).

26. SECRET areas **should** be designated as PED-prohibited areas (ISM control 1169).

27. Commanders and Managers may designate any area to be a PED-prohibited area if they determine the requirement through a risk assessment. The risk assessment should determine the types of PEDs and removable media that are to be prohibited in that area, taking into consideration secure areas and limited access areas, as well as areas that process and store private information.

Example: *Mobile phones and cameras may be prohibited from a specific location such as an aircraft hangar.*

Example: *Equipment capable of recording sound may be prohibited from an area where private counselling is held due to the risk of unintentionally recording private conversations.*

28. PED-prohibited areas are to be clearly sign posted. These signs are to:

a. draw attention to the types of devices that are prohibited from the area; and

b. advise the action that may be taken if unapproved devices are found.

29. Rooms or zones used for regular classified conversations, meetings, briefings, presentations etc. are to be certified and accredited for that purpose (refer to DSPF Principle 14 – *Audio-visual Security*.)

Facility Design and Development (including Greenfield Sites)

30. Project Managers responsible for developing construction security requirements in new facilities and retrofitting of existing facilities are to, in the early stages of planning, obtain security advice from DS&VS or the relevant ESA. Greenfield sites for new projects identified to process, handle and store security-

protected assets are to be categorised and accredited using the Security Zone methodology described above.

Control Requirements

31. Security Zones and risk mitigation control measures guidelines Table 3, provides a combination of a performance-based and prescriptive specification which, when applied, will permit certification of the nominated facilities by the relevant accrediting authority.

32. The risk mitigation control requirements, which are outlined in Physical Security Management Guidelines - Security Zones and risk mitigation control measures and ASIO Technical Note 1-15 are the minimum prescriptions; they may not encapsulate all types of protection required for people and security-protected assets. Where bases or facilities face increased threats, for example terrorism, foreign interference, politically motivated violence, criminal activity etc., a risk assessment is to be conducted to determine additional prescriptions above the minimum for any zone.

Security Clearance Requirements for Access to Security Zones

33. Personnel security clearance requirements for each Zone differ and ultimately are dependent on the classification of any information or asset stored and handled within the Zone. A summary of PSPF security clearance requirements by Zone follows:

a. Zones One and Two - determined by security risk assessment;

b. Zone Three - if security classified official information or assets are held, all employees with ongoing access are to hold a security clearance at the highest level of the information/asset **they access in the Zone**; and

c. Zones Four and Five - if security classified official information or assets are held, all employees with ongoing access are to hold a security clearance at the highest level of the information or asset **held in the Zone**.

Exception: *Zones Three to Five - visitors do not require a specific security clearance as they will be escorted at all times within these Zones.*

Alternate Storage Arrangements for Security Protected Assets

34. Where it is impractical to apply the controls as described in the guidelines, for security-protected assets, (i.e. the shape and size of the asset precludes it from being housed in a building) alternate measures are to be applied that:

a. provide the equivalent level of protection to the requirement being varied;

b. address any specific risk identified in a security risk assessment; and

c. meet the business needs of the asset owner/custodian.

35. Where an asset is classified, it is to be stored in the same way as information of the same classification, refer to *Determining Physical Security Risk Mitigation Measures*, above. Where it is operationally prohibitive or impractical to do so due to the nature of the asset and physical limitations of security containers, classified assets are to be stored in a secure facility that provides an equivalent level of protection afforded to information of the same classification. DS&VS or the relevant ESA can be contacted for advice.

36. Where it is impractical altogether to store classified assets in a secure facility, they are to be protected from unauthorised surveillance and theft. DS&VS or relevant ESA can be contacted for advice. Advice is heavily dependent on the asset and will involve measures to prevent:

a. access by unauthorised persons;

b. surveillance that could reveal classified information about the asset's characteristics or capabilities; or

c. interception of any classified electronic emanations.

37. To prevent unauthorised surveillance of a classified asset it should:

a. be covered in such a way that the shape of the item is disguised and, if possible, be out of sight from any public area; and

b. be protected against an advanced technical intelligence attack by sophisticated surveillance equipment which could include, but is not limited to; optical, acoustic, seismic, magnetic, radar, image intensification, thermal imaging equipment or satellites.

38. If there is a risk of interception of non-communication electronic emanations from a classified asset, such as radars in weapons or surveillance systems, TEMPEST advice is to be obtained from the Australian Signals Directorate.

Storage of High-Risk Unclassified Assets

39. It is recommended that high-risk unclassified assets be stored, where practical, in commercial safes and vaults designed to give a level of protection against forced entry commensurate with the BIL of the asset. Table 2 in Annex A to this DSPF Control, is to be used as a guide to selecting commercial safes and vaults for storing assets.

40. Alternate measures should be used that give the same level of intrusion resistance and delay for assets that cannot be secured in safes or vaults, such as large items or when it is operationally prohibitive (in this case JOC will need to assess and formally accept the risk in accordance with the thresholds for this

DSPF Principle.) It is recommended that personnel consult with a suitably qualified locksmith or vault manufacturer to determine the appropriate safe or vault for their needs.

41. Where it is impractical altogether to store high-risk unclassified assets in a secure facility, they should be protected from unauthorised surveillance and theft. DS&VS or the relevant ESA can be contacted for advice.

Guarding and Patrol Requirements

42. Guards provide deterrence against loss of security-protected assets and can provide a rapid response to security incidents. Guards and patrols may be used separately or in conjunction with other security measures. The requirement for guards, their duties and the need for, and frequency of, patrols should be based on the level of threat and any other security systems or equipment that are already in place. This section is to be read in conjunction with DSPF Principle 75 – *Contracted Security Guards*.

Out-of-Hours Guarding

43. Out-of-hours guarding or patrols may be used instead of alarm systems in Zones Two to Three. These guards may be permanently on site or visit facilities as part of regular mobile patrolling arrangements. There is no requirement for guards to be used in a Zone One, unless a security risk assessment dictates otherwise.

44. Out-of-hours guarding or patrols may be used to supplement a SCEC-approved Type 1(A) SAS in Zones Four and Five, however they are not to be used as a permanent substitute/replacement for the alarm system itself.

Note: *A SCEC-approved Type 1(A) alarm system is a mandated requirement for the certification of Zone Four/Five areas. Guards may be used as a temporary 'stop-gap' measure if the alarm system is non-operational.*

45. Guards should hold security clearances at the highest level of information to which they may reasonably be expected to have incidental contact; refer to DSPF Principle 75 – *Contracted Security Guards* for further details.

Out-of-Hours Patrolling

46. Surveillance is to include after-hours inspection by mobile patrols. Mobile patrols that are used instead of an alarm system, where practical are to check all security cabinets, containers, assets and access points as part of their patrols. If it is impractical to physically check all these items, then the facility itself housing the items is to be physically inspected.

47. If security-protected assets are wholly protected by an operating security alarm system, then patrols of these items should be undertaken at intervals not exceeding 24 hours.

Note: *This would generally be the case for Zones Four and Five, which by their nature, would be wholly protected by an operating security alarm system.*

48. If security-protected assets are not wholly protected by an operating security alarm system, then patrols of these items should be undertaken at random intervals not exceeding:

a. four hours for Zone Three, and

b. based on a security risk assessment for all other Zones.

Note: *BILs should determine the frequency of patrols during the risk assessment process. Assets with higher BIL may require shorter patrol time intervals than assets with lower BIL.*

Security Zones in Areas of Operations

49. The fundamental principles of the Security Zone methodology apply equally to areas of operations. What may differ between operational and domestic Security Zones is the ability to rigidly apply security controls described within the guidelines. 'Defence in depth' and 'force protection' measures applied to an area of operations, may replace the relevant security control described in the guidelines if:

a. it is operationally prohibitive or impractical to apply PSPF prescribed controls (in this case JOC will need to assess and formally accept the risk in accordance with the thresholds for this DSPF Principle); and

b. the control measures applied provide an equivalent level of protection to the security control being varied.

50. This can be considered part of the normal physical security variation process. Variations in areas of operations are to be approved by the relevant Task Force Commander.

Example: *It is impractical to store an asset classified at SECRET in a Zone Three area in accordance with PSPF requirements (constructed to AS3555.1-2003 and surveilled by an AS 2201 Class 5 alarm system.) A variation may be approved to store and handle the asset in a tented area surrounded by barbed wire and permanently guarded by armed personnel, with back up able to attend in less than five minutes, as long as the fundamental access control principle of 'limited Defence personnel and contractor access with escorted visitors only' is applied.*

Australian Defence Force Platforms

51. Australian Defence Force (ADF) platforms, due to varying designs, may not conform to the technical specifications described in the PSPF Security zones and risk mitigation control measures guidelines and ASIO Tech Notes. Asset owners are to apply the variation methodology described within ASIO Technical Note 1-15.

Specific Handling Requirements for Security-Protected Assets

52. **Physical Transfer**. Security-protected assets are to be transported in accordance with DSPF Principle 71 – *Physical Transfer of Information and Assets*.

53. **Accounting**. Security-protected assets are to be accounted for in accordance with the requirements detailed in the Defence Logistics Manual (DEFLOGMAN) Part 2 Volume 5 Chapter 18 Data Quality Management Policy.

54. **Disposal**. Classified assets are to be disposed of in accordance with DSPF Principle 10 – *Classification and Protection of Official Information*. High risk unclassified assets are to be disposed of in accordance with the requirements of DEFLOGMAN Part 2 Volume 5 Chapter 10 Defence Disposal Policy and any Defence instructions specifically related to the asset.

55. **Loss**. The loss of a security-protected asset is a security incident and is to be reported and investigated in accordance with DSPF Principle 77 – *Security Incidents and Investigations* and CEI 6.3 Loss and Recovery of Public Property.

Note: *Early reporting in accordance with DSPF Principle 77 – Security Incidents and Investigations may prevent further compromise and minimise the extent of damage arising from the security incident.*

56. **Special Access Programs**. Additional requirements for the handling of security-protected assets relating to the Defence Special Access Program are detailed in DI(G) Admin 62-1 *Defence Special Access Programs - Policy and Management*.

Roles and Responsibilities

Project Managers

57. Project Managers, who are responsible for construction or refurbishment projects, are responsible for compliance with this DSPF part and the source material it references. For further information regarding project security, refer to DSPF Principle 11 – *Security for Projects*.

Facility Owners

58. Facility owners, including Base Support Managers (BSM), relevant Unit Commanders and Managers, and DISP member facility owners, are responsible for:

a. the identification and categorisation of Security Zones for which they are responsible;

b. base, facility or site planning;

c. controlling access to bases and facilities through the use of appropriate physical security controls;

d. identifying the need and commencing the processes for certification and accreditation; and

e. ensuring that faculties meet the standards required for certification and accreditation and are maintained throughout the life of the accreditation period.

Note: *If the facility owner is a DISP member, that DISP member is responsible for these activities, however, risk ownership remains with the sponsoring Defence Service or Group.*

Asset Custodians

59. Asset custodians are responsible for:

a. factoring the management of security-protected assets for which they are the custodian into their security risk management and planning, refer to the DSPF Governance and Executive Guidance;

b. the physical security procedures within the areas under their control;

c. ensuring that aggregated security-protected assets in their custody are appropriately protected in accordance with this DSPF part; and

d. ensuring that employees or Contractors, Consultants and Outsourced Service Providers working with aggregated security-protected assets are aware of, and comply with the requirements for protecting the asset as detailed in this DSPF Principle.

DISP Members

60. DISP members are responsible for maintaining accreditation of their facilities, including meeting the necessary physical security standards. Defence sponsors retain the security risk associated with outsourced activities and are to monitor DISP contractor processes to ensure physical security standards are maintained. For further information refer to DSPF Principle 16 – *Defence Industry Security Program*.

Contract Managers

61. Contract Managers are responsible for:

a. the acceptance of physical security risks arising from the storage of official information and security-protected assets at Outsourced Service Provider facilities; and

b. ensuring that Defence assets are protected in accordance with this DSPF part when those assets are in the possession of Contractors, Consultants and Outsourced Service Providers.

Key Definitions

62. **Asset custodian**. The Commander or Manager responsible for the protection of asset(s) (including security-protected assets) upon issue to them by the asset owner.

63. **Asset owner**. The Group Head or Service Chief with responsibility and accountability for an asset for which responsibility has been assigned to them.

64. **Business Impact Level (BIL).** A standardised rating that forms part of a security risk management process and identifies the level of impact on Defence and the National Interest resulting from a compromise of confidentiality, loss of integrity or unavailability of individual or aggregated information and assets. Refer to the Australian Government physical security management guidelines, Business impact levels for further information.

65. **Facility owner**. The person responsible for the operation of a facility.

66. **Official Information**. Any information received, developed or collected by, or on behalf of, the Australian Government, through its agencies and Contractors, Consultants and Outsourced Service Providers, that includes:

a. documents and papers;

b. data;

c. software or systems and networks on which the information is stored, processed or communicated;

d. intellectual information (knowledge) acquired by individuals; and

e. physical items from which information regarding design, components or use could be derived.

67. **Security Construction and Equipment Committee (SCEC).** A standing inter-departmental committee which reports to the Protective Security Policy Committee (PSPC). The SCEC is responsible for the evaluation of security equipment for use by Australian Government agencies, and for promulgating the Security Equipment Evaluated Products List (SEEPL).

68. **Security-protected asset**. A non-financial, reportable or accountable asset or information that requires greater than standard fire and theft protection due to either:

a. being allocated a national security classification or Dissemination Limiting Marker (DLM);

Note: *The application of a security classification or DLM indicates that the information or asset has inherent confidentiality requirements.*

b. an unacceptable business impact that would result from the unauthorised modification (i.e. loss of integrity) of the information or asset, irrespective of whether that modification can be detected or not;

c. an unacceptable business impact that would result from the information or asset being unavailable (i.e. loss of availability) for a given period of time; or

d. being categorised as a weapon or explosive ordnance.

69. **Security Zones**. A methodology for physical security mitigation based on a security risk assessment. It is a multi-layered system in which physical security measures combine to provide security-in-depth to those areas on a site that protect assets which require more than normal fire and theft protection.

70. **Technical authority for physical security**. The arbiter for guidance, advice and decision making for technical matters relating to physical security specifications and standards required to achieve certification and accreditation.

71. **TOP SECRET area**. An area certified as a security zone (Zone 4 or 5) approved for handling and storing top secret material.

72. **Variation**. An approved alternate, substitute or risk-mitigated design that meets the intent of physical security standards or specifications.

Note: *Physical security variations apply specifically to standards or specifications described in either ASIO Technical Notes or Defence-specific technical guidance presented in this DSPF part. They are used when it is impractical to meet the prescribed standard or specification.*

73. **Greenfield**. In the physical security context, a Greenfield site is a property that has not undergone an Australian Government security treatment.

Further Definitions

74. Further definitions for common PSPF terms can be found in the Glossary

75. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A — *Security Containers, Vaults and Safes*

Annex B — *Policy Transition from Security Rated Areas to Security Zones*

Document Administration

Identification

DSPF Control	Physical Security
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)
DSPF Number	Control 72.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Physical Security
Related DSPF Control(s)	N/A

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 SPS	Launch

Defence Security Principles Framework (DSPF)

Annex A to Physical Security – Security Containers, Vaults, and Safes

Security Containers for Official Information

1. Information originators are to determine the appropriate Business Impact Level (BIL) for official information in accordance with Business Impact Levels guidelines.

2. The Physical Security Management Guidelines: Security Zones and Risk Mitigation Control Measures provide Whole of Australian Government guidelines on the physical controls required to protect assets (including information).

a. In accordance with the Protective Security Policy Framework (PSPF), Defence is required to select the minimum level of security containers or security rooms for storing official information where the compromise, loss of integrity or unavailability of the information has a business impact level. Table 1 should be used when selecting the minimum level of security containers or security rooms. Information with a Sensitive DLM will have specific handling requirements detailed in a footer or cover page to the document. If these handling requirements exceed the requirements of this table, the higher requirement is to be applied.

b. Secured from unauthorised access means the information can be stored in containers other than a specified security container, for example - a desk drawer or cabinet. The information is to be stored discreetly and secured from casual access.

   In exceptional circumstances to meet an operational requirement—for example, where TOP SECRET information cannot be returned to a Zone Five area—personnel may store TOP SECRET information for a period not to exceed five days in a Zone Three or Four area. Advice from ASIO-T4 should be sought before implementing arrangements for the temporary storage of TOP SECRET information outside a Zone Five area.

Table 1 – Security Containers for Official Information

Classification / Business Impact Level	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Unclassified official information the compromise, loss of integrity or unavailability of which would have a BIL of 1 (Low).	Locked commercial container	Secured from unauthorised access (see note b)	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access
Aggregated information the compromise, loss of integrity or unavailability of which would have a BIL of 1 (Medium). Or limited holdings of information with an FOUO or Sensitive DLM (see note a)	Security Construction and Equipment Committee (SCEC) Class C	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access
Aggregated information the compromise, loss of integrity or unavailability of which would have a BIL of 2 (High). Or limited holdings of PROTECTED information	Ongoing storage not recommended, if unavoidable SCEC Class C	SCEC Class C	SCEC Class C	Container to be determined by a security risk assessment	Container to be determined by a security risk assessment

Classification / Business Impact Level	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Aggregated information the compromise, loss of integrity or unavailability of which would have a BIL of 3 (Very High). Or limited holdings of CONFIDENTIAL information	Not permitted	SCEC Class B	SCEC Class C	SCEC Class C	Container to be determined by a security risk assessment
Aggregated information the compromise, loss of integrity or unavailability of which would have a BIL of 4 (Extreme). Or limited holdings of SECRET information	Not permitted	SCEC Class A	SCEC Class B	SCEC Class C	SCEC Class C
TOP SECRET classified information the compromise, loss of integrity or unavailability of which would have a BIL of 5 (Catastrophic)	Not permitted	Not permitted	Not normally permitted. (In exceptional circumstances SCEC Class A) see note c	Not normally permitted. (In exceptional circumstances SCEC Class B) see note c	SCEC Class B

Safes and Vaults for Protection of High Risk Unclassified Assets

3. It is recommended that security-protected assets be stored, where practical, in commercial safes and vaults designed to give a level of protection against forced entry commensurate with the business impact level of the asset. In accordance with the PSPF, Defence is required to select the minimum level of security containers or security rooms for storing official information where the compromise, loss of integrity or unavailability of the information has a business impact level. Table 2 is to be used as a guide to selecting commercial safes and vaults for storing assets.

Note: *For the purposes of transition, Table 2 references the former asset categories together with the business impact levels for high risk unclassified assets.*

Table 2 – Selecting Safes or Vaults to Protect High Risk Unclassified Assets (GUIDANCE ONLY)

High risk unclassified assets / categorised assets	**Zone One**	**Zone Two**	**Zone Three**	**Zone Four**
High risk unclassified assets the loss of which would have a BIL of 1 (Low-Medium) or SUPPORT assets	Locked commercial container	Locked commercial container	Determined by a security risk assessment	Determined by a security risk assessment
High risk unclassified assets the loss of which would have a BIL of 1 (Low-Medium) or SENSITIVE and ATTRACTIVE assets	Commercial safe or vault	Determined by a security risk assessment	Determined by a security risk assessment	Determined by a security risk assessment
High risk unclassified assets the loss of which would have a BIL of 2 (High) or IMPORTANT assets	Commercial safe or vault	Commercial safe or vault	Commercial safe or vault	Determined by a security risk assessment
High risk unclassified assets the loss of which would have a BIL of 3 (Very High) or MAJOR assets	AS 3809 commercial safe or vault	Commercial safe or vault	Commercial safe or vault	Commercial safe or vault
High risk unclassified assets the loss of which would have a BIL of 4 (Extreme)	AS 3809 high security safe or vault	AS 3809 medium security safe or vault	AS 3809 commercial safe or vault	Commercial safe or vault
High risk unclassified assets the loss of which would have a BIL of 5 (Catastrophic)	Should not be held unless unavoidable	Should not be held unless unavoidable	AS 3809 high or very high security safe or vault	AS 3809 medium or high security safe or vault

Use of Security Containers

4. Commanders and managers are **must** maintain a register of all security containers, combinations and keys. Each container **must** have a custodian who is responsible for its contents and controlling access to the container. Table 3 outlines the processes for the use of security containers.

Table 3 – Use of Security Containers

Aspect	Procedure
Unlocked containers	When unlocked, the door is to be kept open, bolt returned to the locked position, and the key is to be removed, if applicable.
Closed doors or drawers	Are to be locked when the doors or drawers are closed.
Access to locks	**Must** be sealed on installation and after repair, so that access to the back of the lock is not possible.
Combination locks	**Must** not be opened in view of people who are not authorised to know the combination.
Labels	Are not to be placed near locks, bolts or hinges to ensure that signs of tampering or unauthorised entry are visible. Labels are not to give any indication of the contents of the container. 'Open/closed' labels are not to be used.
Keys	The security officer will: a. hold all duplicate keys when the container (including Class C rooms) is locked; and b. maintain a key register.

Movement

5. Prior to relocating a security container, the security officer **must** be advised. When relocating a security container, a risk assessment will determine if the container is to be completely emptied of all documents and if any labels attached to the inside are to be removed.

6. The locking pins **must** be reinserted if it is a Class A container.

Disposal

7. Before a container is returned to the store, it **must** be completely emptied of all documents and have a signed certificate attached to its body stating that it has been emptied and checked. The process is to include removing and replacing drawers to ensure that no classified items have been concealed behind or below drawers.

8. The key register must be updated to reflect the change. Additionally:

a. for a keyed lock container, keys will be removed and sent to the store separately with details of their container; or

b. for a combination lock container:

   i. the lock **must** be reset to the manufacturer's standard setting (usually 40-50-60 or as shown in the instruction book); and

   ii. the combination **must** be marked on the outside of the container.

Note: *Disposal must be conducted via a Defence approved disposal authority*

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Security Containers, Vaults and Safes
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Physical Security
DSPF Number	Control 72.1

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 SPS	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B to Physical Security – Policy Transition from Security Rated Areas to Physical Security Zones

Transition from Security Rated Areas to Physical Security Zones

1. The PSPF has amended the physical security methodology, replacing the former Security Rated Areas with Physical Security Zones. To facilitate a smooth transition between methodologies, the following policy is provided.

Existing Certification for Security Rated Areas

2. Table 1 has been developed for those areas holding a certification/accreditation certificate describing a 'Security Rated Area'; Refer DSPF Principle 73 – *Facilities Certification and Accreditation*.

3. If a certified/accredited Security Rated Area meets the requirements of Table 1 and holds a current accreditation certificate with no changes to the physical structure or supporting procedures, it may be deemed an accredited Physical Security Zone by the appropriate accreditation authority. All requests for an updated accreditation certificate must be supported by a statement that there has been no change to physical controls or an increase in threat since the original certification/accreditation was issued. If the accrediting authority agrees to the change, the accreditation certificate is to be updated to reflect the change to the Physical Security Zone methodology.

Table 1 – Transitional Arrangements

If the Security Rated Area is:	And access control measures provide…	It equates to a Physical Security Zone of…
Public Access/Unsecure Area	Unfettered access to members of the public	Zone One
Accredited Intruder Resistant Area	Unrestricted Defence personnel, Contractor, Consultant and Outsourced Service Provider access; and Restricted public access	Zone Two
Accredited Partially Secure Area	Limited Defence personnel, Contractor, Consultant and Outsourced Service Provider access and escorted visitors only	Zone Three
Accredited Secure Area	Strictly controlled Defence personnel, Contractor, Consultant and Outsourced Service Provider access and escorted visitors only with an identified need to be there	Zone Four
Accredited TOP SECRET Areas	Strictly controlled Defence personnel, Contractor, Consultant and Outsourced Service Provider access and escorted visitors only with an identified need to be there	Zone Five

Interim Physical Security Zones

4. Some areas or facilities cannot be considered an official Physical Security Zone without completing a full accreditation process, refer DSPF Principle 73 – *Facilities Certification and Accreditation*. These include areas of facilities that:

a. do not hold a current accreditation certificate;

b. hold an accreditation certificate, but do not meet the minimum access control requirements; or

Example: *The entirety of a building is considered a Secure Area, but its outer perimeter borders a public access area. During business hours, members of the public may access the foyers of the building, and there is unlimited access by Defence personnel, Contractors, Consultants and Outsourced Service Providers access to all common areas of the building (such as stairwells, elevators and open office environments.) Under the Physical Security Zone methodology, the entirety of the building can no longer be considered a Zone Four during business hours.*

c. are not current Security Rated Areas, but process, handle and store high-risk unclassified assets.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Policy Transition from Security Rated Areas to Physical Security Zones
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Physical Security
DSPF Number	Control 72.1

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 SPS	Launch

Defence Security Principles Framework (DSPF)

Physical Security Certification and Accreditation

General principle

1. Defence conducts physical certification and accreditation processes to ensure that Defence's information, Security Protected Assets and infrastructure are protected by the necessary measures to meet identified security risks

Rationale

2. The certification and accreditation process enables Defence to manage security risks to classified information, Security Protected Assets and infrastructure. Accreditation of facilities provides the confidence Defence Groups and Services, and other Government agencies (domestic and foreign) need in order to share information and Security Protected Assets with each other or Industry partners.

Expected outcomes

3. Certification of facilities is conducted as part of every accreditation and re-accreditation process.

4. Defence conducts certification of facilities against Defence Security Principles Framework (DSPF) and Protective Security Policy Framework (PSPF) security standards, and is consistent with Whole-of-Government direction on protective security.

5. The accreditation authority reviews the outcomes of the certification process, and confirms appropriate mitigation measures are in place. Where applicable, the accreditation authority assesses whether appropriate risk management has been undertaken by control officers to determine if the residual risk to a facility is acceptable to Defence and, if so, provide authority to operate.

6. Facilities are re-accredited at intervals specified within Control 73.1 - *Physical Security Certification and Accreditation*, and when;

a. changes occur to the Business Impact Levels associated with the ICT systems or assets handled or stored in the facility;

b. significant changes to the tenancy and governance arrangements, architecture of the facility or physical security controls used at the facility occur; or

c. requested by DS&VS or the facility owner.

7. Accreditation authorities temporarily or permanently revoke accreditation on security grounds if they believe the risk of operation to a facility is unacceptable to Defence.

Escalation Thresholds

Risk Rating	Responsibility
Low	APS 6/O-4 – Security Adviser or delegate of relevant equivalent Executive Security Adviser (ESA)
Moderate	EL 1/O-5 – DS&VS Security Manager or delegate of relevant equivalent ESA
Significant	EL 2/O-6 – Director Security Services or delegate of relevant equivalent ESA through EL 1/O-5
High	EL 2/O-6 - Director Security Services or delegate of relevant equivalent ESA
Extreme	Assistant Secretary Security Policy and Advice (AS SPS)

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Note: *The above Escalation Thresholds are for domestic application. 'Defence in depth' and 'force protection' measures applied to an area of operations may replace relevant controls in the DSPF if:*

a. it is operationally prohibitive or impractical to apply DSPF and PSPF prescribed controls (in this case JOC will need to assess and formally accept the risk in accordance with the thresholds for this Principle); and

b. the control measures applied provide an equivalent level of protection as the security control being varied.

Document administration

Identification

DSPF Principle	Physical Security Certification and Accreditation
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 73
Version	2
Publication date	17 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 73.1
Control Owner	Assistant Secretary Policy and Advice (AS SPS)

Related information

Government Compliance	**PSPF Core Requirements:** Entity Facilities; and Entity Physical Security.
Read in conjunction with	N/A
See also DSPF Principle(s)	Personnel Security Clearance Classification and Protection of Official Information Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Physical Transfer of Official Information, Security Protected and Classified Assets Physical Security Access Control
Implementation Notes, Resources and Tools	Australian Government physical security management guidelines—Security zones and risk mitigation control measures

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	17 July 2018	FAS S&VS	Corrected Control Owner designation

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Physical Security Certification and Accreditation

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this enterprise wide control.

Escalation Thresholds

Risk Rating	Responsibility
Low	APS 6/O-4 – Security Adviser or delegate of relevant equivalent Executive Security Adviser (ESA)
Moderate	EL 1/O-5 – DS&VS Security Manager or delegate of relevant equivalent ESA
Significant	EL 2/O-6 – Director Security Services or delegate of relevant equivalent ESA through EL 1/O-5
High	EL 2/O-6 - Director Security Services or delegate of relevant equivalent ESA
Extreme	Assistant Secretary Security Policy and Advice (AS SPS)

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Note: *The above Escalation Thresholds are for domestic application. 'Defence in depth' and 'force protection' measures applied to an area of operations may replace relevant controls in the DSPF if:*

a. it is operationally prohibitive or impractical to apply DSPF and PSPF prescribed controls (in this case JOC will need to assess and formally accept the risk in accordance with the thresholds for this Principle); and

b. the control measures applied provide an equivalent level of protection as the security control being varied.

Facilities Needing Accreditation

2. Defence and Defence industry facilities that **must** be accredited are:

a. Security Zones that process, handle or store:

i. classified information PROTECTED and above;

ii. Security Protected Assets with a Business Impact Level (BIL) of 2 (high) and above;

iii. ICT systems PROTECTED or above that are not protected by Australian Signals Directorate (ASD) endorsed encryption; and

iv. aggregated information with a BIL of 2 (high) and above;

Note: *Facilities that do not process, handle or store security-protected assets (ie. assets that do not attract a BIL and thus only require standard fire and theft protection), are not categorised as a Security Zone and therefore do not require accreditation.*

Note: *ICT system accreditation is undertaken separately to physical accreditation and is required for each system that operates in an accredited Security Zone. Refer to DSPF Principle 23 – ICT Certification and Accreditation.*

b. armouries and licenced explosive ordnance facilities;

c. facilities where technical surveillance countermeasures are implemented (eg. Audio Secure Rooms); and

d. joint and allied facilities subject to relevant legislation, a General Security Agreement (GSA), a Security of Information Agreement or Arrangement (SIA) or a memorandum of understanding.

Note: *DS&VS can confirm whether or not a GSA, a SIA or a memorandum of understanding is in place that would affect joint or allied facilities.*

3. Defence and Defence industry facilities that store security-protected assets with BILs of low-medium, or house ICT systems operating at the UNCLASSIFIED (including UNCLASSIFIED Dissemination Limiting Marked (DLM) information) level (BILs low-medium); are to be risk assessed by the Control Officer (in consultation with the relevant accreditation authority), to determine if the facility is to be subject to a physical accreditation.

Exclusion: *A company that is processing For Official Use Only (FOUO) material that is solely related to the company's business dealings with Defence does not require a facility accreditation.*

Physical Certification and Accreditation Authorities

4. The following facilities and security zones **must** be certified and accredited by the authorities identified in Table 1 of this Control, unless an alternative is approved by the AS SPS:

Table 1 – Physical Certification and Accreditation Authorities

Facility	Location	Physical certification authority	Physical accreditation authority
Domestic - Security Zones One through to Four (including off-site areas such as home-based areas)	Joint, non-Service unit or DISP member's facilities.	DS&VS	DS&VS
Domestic - Security Zones One through to Four (including off-site areas such as home-based areas)	Single-Service Unit.	SSA(f)	SSA
Domestic – Commercial Shared Data centre facilities	In Australia on industry premises.	DS&VS	DS&VS
Domestic - Security Zone Five, not including SCI	All Defence and Defence industry/DISP members.	ASIO T4(g)(i)	DS&VS
Domestic - Security Zone Five, not including SCI	Single-Service unit.	ASIO T4(g)(i)	SSA
Domestic - Compartments within Zone Five	Joint, non-Service unit facility or DISP member's facility.	DS&VS	DS&VS
Domestic - Compartments within Zone Five	Single-Service unit.	SSA(f)	SSA

Facility	Location	Physical certification authority	Physical accreditation authority
Domestic - SCI	All Defence and Defence industry/DISP members.	ASIO T4(g)(i)	DIS to coordinate
Armoury or licensed EO facilities (refer to DSPF Principle 78 –Weapons Security and DSPF Principle 79 – Explosive Ordnance Security)	Joint, non-Service unit facility or DISP member's facility.	DS&VS	DS&VS
Armoury or licensed EO facilities (refer to DSPF Principle 78 –Weapons Security and DSPF Principle 79 – Explosive Ordnance Security)	Single-Service unit.	SSA(f)	SSA
Armoury or licensed EO facilities (refer to DSPF Principle 78 –Weapons Security and DSPF Principle 79 – Explosive Ordnance Security)	Supporting an operation.	CJOPS(b)	CJOPS(b)
ADF Platforms	In Service or regular maintenance.	SSA(h)	SSA(h)
Overseas - All Security Zones	In an Australian Diplomatic Mission.	DFAT(a)	DFAT(a)
Overseas - All Security Zones	Supporting an operation.	CJOPS(b)	CJOPS(b)
Overseas - All Security Zones	External to an Australian Diplomatic Mission (excluding deployments).	The DS&VS(c) to coordinate(d) Note: The DS&VS consults with DFAT and local accreditation authorities in accordance with SIAs	The DS&VS(c) to coordinate(d) Note: The DS&VS consults with DFAT and local accreditation authorities in accordance with SIAs

Facility	Location	Physical certification authority	Physical accreditation authority
Overseas - All Security Zones	Physical Security Zone Five (not including SCI) and compartments within Zone Five - External to an Australian Diplomatic Mission.	DS&VS to coordinate	DS&VS
Overseas - All Security Zones	SCI - All Defence and Defence industry/DISP members in and external to Australian Diplomatic Missions.	DIS(e) to coordinate	DIS(e) to coordinate

Notes to Table 1:

(a) Department of Foreign Affairs and Trade (DFAT)
(b) Chief of Joint Operations (CJOPS)
(c) Defence Security and Vetting Service (DS&VS)
(d) On occasions, the DS&VS may delegate certification responsibility to the Chief Information Officer Group (CIOG), where CIOG is attending an overseas location to certify an ICT system
(e) Defence Intelligence Security (DIS)
(f) Air Force Protective Security and Governance conduct certification activities for Air Force units
(g) Certification activities undertaken by the Australian Security Intelligence Organisation (ASIO) are conducted on a cost-recovery basis. All liaisons between ASIO T4 and Defence in relation to the certification and accreditation of Defence TOP SECRET facilities, including the management of arrangements for TSCM, are managed by the DS&VS.
(h) Consideration is to be given to service or platform specific policies and applicable Operating Procedures (including emergency destruction) and any physical limitations.
(i) AE851 – Request for T4 Certification of a Zone 5/SCIF Defence site.

Process

Facility Certification

Prior to Certification

5. Certification is to be conducted as part of every facility accreditation or reaccreditation. Facility and asset owners are required to apply the minimum security controls detailed in the DSPF (refer to DSPF Principle 72 – *Physical Security*) as determined by the BIL of the assets being protected and consideration of security risks to the asset(s). It is recommended that facility or asset owners contact the certification authority to confirm physical security requirements prior to conducting any infrastructure work. For infrastructure projects, it is recommended that consultation occur during planning and design phases stages.

Minimum Physical Security Standards

6. Minimum physical security controls outlined in the DSPF (refer to DSPF Principle 72 – *Physical Security*) are risk-based measures aligned with the PSPF. Application of minimum security controls provides assurance across Defence and other government agencies that a consistent set of controls are applied for the protection of assets.

7. Physical certification authorities will assess the level to which a facility complies with the minimum controls identified in:

a. DSPF Principle 72 – *Physical Security* for all Physical Security Zones, including all standards referenced from it;

b. Annex C to DSPF Control 78.1 – *Weapons Security* for armoury standards; and

Note: *See DSPF Control 79.1 – Explosive Ordnance Security for information regarding security standards for licensed explosive ordnance facilities.*

c. DSPF Control 14.1 – *Audio-visual Security* for Audio Secure Room standards, including all standards referenced from it.

If Minimum Security Controls are Met

8. If the minimum security controls are met, the certification authority will:

a. certify the facility as having achieved the minimum standard required; and

b. document the outcome of the certification in a formal report.

If Minimum Security Controls are Not Met

9. During the certification process, the facility or asset owner, or the certification authority may identify that minimum security controls have not been met or inappropriate security controls applied. In such circumstances the facility or asset owner has the option to either rectify the deficiency by applying the appropriate security control(s) or, undertake a security risk process if departing from the required standard to identify alternate controls in consultation with the certification authority. For guidance on risk management in the DSPF, refer to DSPF *Governance and Executive Guidance*.

If Additional Security Controls are Required

10. Unless specified in a Defence Instruction or International Security Agreement, the need for additional security controls above the minimum standard (refer to DSPF Principle 72 – *Physical Security*) is to be substantiated through a formal security risk management plan.

Certification Documents

11. Where applicable, the certification authority needs to receive the following documentation from facility or asset owners so certification can be provided:

a. Confirmation of surveillance arrangements, such as:

   i. a Type 1A SAS commissioning certificate issued by a Security Construction and Equipment Committee (SCEC) Security Zone Consultant;

   ii. an installation certificate for a commercial alarm system, which states compliance with AS2201 (not applicable for Zones Four or Five); or

   iii. guarding and after-hours patrol procedures for the facility, or a combination of SAS and guard patrols.

b. an electronic access control system certification from suitably qualified system installers or designers (required for Security Zones Three, Four and Five; required only if installed in Security Zones One or Two);

c. any treatment plan for controls required above the baseline requirements; and

d. any other documentation requested by the certification authority.

Accreditation

12. Accreditation is the process undertaken by an authority providing formal recognition that certification requirements have been met and risks adequately assessed and addressed by facility and/or asset owners. Once satisfied that risks have been appropriately addressed, the accreditation authority will issue an accreditation certificate to the facility owner permitting operation of a facility.

13. Accreditation cannot be awarded where departures from necessary security controls are outstanding or have not been approved; or if the residual risk (as determined through the security risk management process) to Defence's people, information, security-protected assets and infrastructure is considered unacceptable. Any recommendation or decision to prevent or suspend accreditation needs to be justified by the accreditation authority, recorded and communicated to the appropriate facility and asset owner(s).

Accreditation Documents

14. If applicable, the accreditation authority is to receive the following certification reports and documentation before the accreditation process can commence:

a. a certification report stating the Security Zone rating of the facility;

b. confirmation that a trained and qualified security officer is appointed for the facility;

c. up-to-date and authorised Security Standing Orders;

d. confirmation that a Security Register is in place for the facility;

e. confirmation that official information is stored in appropriate security containers within the certified Security Zone;

f. an Acoustic Engineer's Report stating the acoustic rating of the facility;

g. a Technical Surveillance Counter Measures certification report for the facility; and

h. a copy of an approved Security Risk Management plan documenting that the security controls for the facility provide adequate protection against identified security risks.

Maintaining Accreditation

15. Accredited facilities are to maintain the standard to which they are accredited. Facility owners are to conduct periodic reviews and self-assessments of the accredited security measures. Annual Protective Security Self Assessments (using form AC064) provide ongoing assurance to Commanders, Managers and DISP member executives that accreditation standards are maintained and identify any remediation where required.

Revoking Accreditation

16. The accreditation authority can temporarily or permanently revoke an accreditation on security grounds if the risk of operation to a facility is found to be unacceptable to Defence. If an accreditation is revoked, the accreditation authority is to document and record the basis for the decision and notify the FAS S&VS before accreditation is revoked.

17. Where accreditation is revoked or not renewed, the accreditation authority will recommend that a facility not operate until the control officer has rectified identified deficiencies or treated risks to an acceptable level. Facility Owners and / or Control Officers retain responsibility for the operation of a facility, including the management of security risks to assets for which they are accountable. In circumstances where an accreditation authority revokes or suspends accreditation, Facility Owners and /or Control Officer's will determine whether a facility will operate, and is required to advise the accreditation authority and relevant stakeholders of their decision.

Reaccreditation

18. Accreditation is not permanent. Reaccreditation of facilities is necessary to provide ongoing assurance that security measures are appropriate for the protection of assets and may be triggered by a number of circumstances including:

a. significant changes in security policies or standards;

b. changes to Defence's security risk profile and/or appetite;

c. expiry of the accreditation due to the passage of time;

d. changes in the BILs associated with the assets handled or stored within a facility;

e. significant changes to the architecture of the facility or the physical security controls used; or

f. a major security incident affecting the facility; and

g. any other conditions stipulated by the accreditation authority.

19. Accredited facilities **must** be reaccredited:

a. When circumstances change, including:

   i. changes to the BILs associated with the ICT system, information or assets handled or stored within;

   ii. significant changes to the tenancy;

   iii. changes in governance arrangements; or

   iv. architecture of the facility or the physical security controls used.

b. At regular intervals as per Table 2, below.

Table 2 –Reaccreditation intervals

Facility	Reaccreditation interval
Zone Two to Four	Only when circumstances change
Zone Five	Three Years
Armouries/Licensed EO facilities	Five Years

Note: *Annual Protective Security Self Assessments (using form AC064) provide ongoing assurance to Commanders, Managers and DISP member executives that accreditation standards are maintained and identify any remediation where required.*

Roles and Responsibilities

First Assistant Secretary Security and Vetting Service (FAS S&VS)

20. The FAS S&VS is responsible for:

a. determining the certification standards for the physical security of Defence facilities (including the certification standards for the physical security of ICT systems in accordance with the Information Security Manual (ISM);

b. recording the physical accreditation status of all facilities accredited by Defence accreditation authorities in accordance with this DSPF part;

c. certification and accreditation assessment of facilities;

d. liaising with the Defence Intelligence Security (DIS) Sensitive Compartmented Information Facility (SCIF) Accreditation Management Team regarding the management and conduct of certification and accreditation of Defence facilities requiring DIS input.

Defence Accreditation Authorities

21. The accreditation authority is responsible for:

a. accrediting facilities and systems assigned to them in accordance with this DSPF Principle;

b. undertaking an independent review of the certifying authority's report and other necessary documentation to determine that the associated residual security risk of a facility is accepted by facility and /or asset owners;

Note: *Accreditation authorities are not obliged to accept the recommendation of a certification report, however if they choose not to do so they are responsible for documenting the basis of the decision.*

c. granting or denying accreditation for the operation of a facility;

d. providing the appropriate risk steward(s) with an accreditation certificate stipulating their responsibilities and accreditation conditions; and

e. recording the details of accreditations and denials.

Department of Foreign Affairs and Trade (DFAT)

22. DFAT is responsible for the physical certification within all Australian missions overseas.

Australian Security Intelligence Organisation (ASIO)

23. ASIO is responsible under whole-of-government arrangements for the physical certification of domestic TOP SECRET facilities and outsourced data centres.

Director Defence Intelligence Organisation

24. On behalf of the DDIO, the DIS SCIF Accreditation Management Team is responsible for accrediting facilities that contain some allied systems and which have a requirement to handle, store, process and discuss Sensitive Compartmented Information (SCI).

Facility and System Owners

25. The Facility or System Owner is responsible for:

a. identifying the need for certification or accreditation;

Note: *DISP Sponsors will undertake this on behalf of DISP members; refer to DSPF Principle 16 - Defence Industry Security Program.*

---

b. the timely engagement of the relevant certification or accreditation authorities, including an indication of the assessed BILsof the asset, and providing support to the authority during the conduct of the certification or accreditation process;

c. where required, providing a security risk management plan to the relevant certification or accreditation authority;

d. developing the necessary supporting documentation described in this DSPF part that are required to successfully complete certification and accreditation;

e. identifying funding arrangements, and whether any 'building' works are scheduled before certification is conducted;

f. ensuring that facilities meet the standards required for certification or accreditation;

g. where required, identifying the need for variations to minimum physical security standards (refer to DSPF Principle 72 - *Physical Security*);

h. maintaining accreditation; and

i. reporting changes in security risk (including, but not limited to, physical and ICT security, operations and security governance), to the appropriate risk owner, accreditation authority and requesting reaccreditation if required.

Commanders and Managers

26. Commanders and Managers are responsible for ensuring facilities meet and maintain certification and accreditation standards. Conducting Annual Protective Security Self Assessment's, using form AC064, will provide ongoing assurance that accreditation requirements are maintained and identify any remediation where required.

Certification authorities

27. The certification authority is responsible for:

a. assessing and certifying facilities against relevant security controls, or variations to those controls, as detailed in the DSPF (refer DSPF Principle 72 - *Physical Security*), and recording the details in a certification report.

b. issuing the certification report along with recommendations to the accreditation authority, detailing the extent to which a facility complies with the relevant Security Zone standard for the assets requiring protection.

28. In relation to their certification role, certification authorities are to provide timely advice and assistance to facility owners to help identify:

a. security zone requirements;

b. instances of non-compliance;

c. remediation strategies, security-in-depth and alternative controls or variations that may be available to mitigate security risks; and

d. requirements for the development of a security risk management plan where necessary.

Key Definitions

29. **Accreditation**: The process by which an authoritative body gives formal recognition that required security standards have been satisfied and, where applicable, associated residual risks have been accepted by a facility and/or asset owner for the operation of a facility. The outcome of the accreditation process is an authority to operate for a particular facility and/or, asset.

30. **Accreditation Authority**: The authority delegated to accredit a facility for use.

31. **Accreditation Certificate**: The formal instrument that:

a. is signed by the accreditation authority confirming that appropriate security measures are in place for the protection of Defence assets and manage identified security risks; and

b. stipulates the conditions under which the facility or asset may operate without requiring a reassessment of the residual risk (by seeking re-accreditation).

32. **Certification**: A formal assurance process resulting in a statement (certification report) that outlines the extent to which a facility conforms to controls for the required Security Zone, and as required by the DSPF. Certification considers any additional controls identified by facility owners as part of a security risk management plan, and ensures appropriate security risk mitigation is applied for the protection of operations, assets and systems handled/stored/processed within the facility.

33. The outcomes of the certification process provide:

a. assurance to facility owners that appropriate security mitigations have been applied for the assets requiring protection; and

b. information to the accreditation authority they require to make an informed decision on whether, from a security perspective, the facility should be approved to operate.

34. **Certification Authority**: A subject matter expert who assess a facility against relevant security controls, which may involve review of security risk management plans provided by facility owner(s) where additional controls to baseline requirements of the DSPF are required.

35. **Certification Report**: The instrument produced by the certification authority that documents the extent to which a facility complies with relevant standards, taking into consideration baseline controls and additional controls subject to security risk management plans, where . The certification report identifies each standard and assesses the degree to which each element of the standard has been achieved.

36. **Security Zones**: A methodology for the application of physical security measures, principally based on an assets Business Impact Level and, where necessary, a security risk management plan. It is a multi-layered system in which physical security measures combine to provide security-in-depth to those areas on a site that protect assets requiring more than normal fire and theft protection.

37. **Facility**: An area that facilitates government business.

Example: *A facility can be a building, storage area floor of a building or a designated space on the floor of a building.*

38. **Facility owner**: The person responsible for the operation of a facility.

39. **System**: A related set of hardware and software used for the processing, storage or communication of information and the governance framework in which it operates. A system can range from a single device such as a laptop, to a Defence-wide network.

40. **Security Protected Asset**: A non-financial, reportable or accountable information or asset that requires greater than standard fire and theft protection due to either:

a. being allocated a national security classification or dissemination limiting marker (DLM);

Note: *The application of a security classification or DLM indicates that the information or asset has inherent confidentiality requirements.*

b. an unacceptable business impact that would result from the unauthorised modification (ie. loss of integrity) of the information or asset, irrespective of whether that modification can be detected or not;

c. an unacceptable business impact that would result from the information or asset being unavailable (ie. loss of availability) for a given period of time; or

d. being categorised as a weapon or explosive ordnance.

41. **Asset owner**: The Group Head or Service Chief with responsibility and accountability for an asset for which responsibility has been assigned to them.

42. **Asset custodian**: The Commander or Manager responsible for the protection of asset(s) on issue to them.

Further Definitions

43. Further definitions for common PSPF terms can be found in the Glossary.

44. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments

Document Administration

Identification

DSPF Control	Physical Security Certification and Accreditation
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)
DSPF Number	Control 73.1
Version	3
Publication date	6 August 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Physical Security Certification and Accreditation
Related DSPF Control(s)	Personnel Security Clearance Classification and Protection of Official Information Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security ICT Certification and Accreditation Physical Transfer of Official Information, Security Protected and Classified Assets Physical Security Access Control

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 SPS	Launch
2	17 July 2018	AS SPS	Corrected Control Owner designation and modified Table 1 to include ASIO T4 form.
3	6 August 2018	AS SPS	Giving CJOPS authority over EO storage and Armouries in areas of Ops.

Defence Security Principles Framework (DSPF)

Access Control

General principle

1. Defence-controlled areas are only to be accessed by persons whose identities have been established and who have the right and requirement to be there.

Rationale

2. Unauthorised access to Defence-controlled areas can lead to:

a. dangers to Defence personnel, Contractors, Consultants and Outsourced Service Providers;

b. theft of and damage to Defence assets and infrastructure; and

c. unauthorised access to sensitive Defence information, and information and communication technology (ICT) systems.

3. Each of these could compromise national security and personal safety.

Expected outcomes

4. Defence controls access to areas that are not designated as public areas. These include restricted Defence bases, establishments, military or business units, defence industry facilities and the assets and systems contained therein or parts thereof.

5. Personnel accessing Defence assets, information and facilities have been identified to have an accepted reason for seeking that access, and where applicable, the appropriate security clearance.

6. Records are retained about persons who have been granted access to Defence assets, information and facilities.

7. Defence is to issue credentials that convey an individual's clearance levels and under what circumstances they have been granted access.

8. Access to Defence assets, information and facilities is revoked for personnel who no longer meet clearance, need-to-know or suitability requirements.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations
Significant	Director General (DG) ESD
High	Defence Security Committee (DSC) – through First Assistant Secretary Service Delivery Division (FAS SD)
Extreme	DSC – through FAS SD

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Access Control
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 74
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 74.1
Control Owner	DG ESD

Related information

Government Compliance	**PSPF Core Requirements**: Eligibility and suitability of personnel; and Entity physical resources. **Legislation**: *Privacy Act 1988 (Cth*
Read in conjunction with	N/A
See also DSPF Principle(s)	Classification and Protection of Official Information Defence Industry Security Program Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Personnel Security Clearance Physical Security Identification, Search and Seizure Regime Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Government physical security management protocol ASIO, Security Equipment Guides (SEGs) are available to ASAs from the GovDex Protective Security Community

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

Defence Security Principles Framework (DSPF)

Access Control

Control Owner

1. The Director General Estate and Service Delivery (DG ESD) (Estate and Infrastructure Group) is the owner of this enterprise-wide control.

Escalation Thresholds

2. The DG ESD has set the following general threshold 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 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations
Significant	DG ESD
High	Defence Security Committee (DSC) – through First Assistant Secretary Service Delivery Division (FAS SD)
Extreme	DSC – through FAS SD

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Control

Identity Management

3. All individuals are to be positively identified prior to gaining entry to any part of a Defence base that is not designated a public access area (Zone 1). Individuals who cannot be positively identified will be denied entry.

Exclusion: *Emergency services personnel, who are attending an emergency incident on a part of a Defence base that is subject to access control arrangements are not required to be positively identified prior to gaining entry.*

Note: *It is recommended that emergency response arrangements are addressed in base security documentation. At larger bases this may include making provision to assist emergency services personnel by escorting them to the site of the incident.*

4. The following groups of people can be identified by their Defence Common Access Cards (DCAC) or Defence issued identity cards, either visually or through Electronic Access Control Systems (EACS):

a. Defence personnel (Australian Public Service (APS) and Australian Defence Force (ADF));

b. ADF and APS family members;

c. APS employees of other Australian Government departments or agencies;

d. authorised foreign nationals;

e. Contractors, Consultants and Outsourced Service Providers; and

f. appropriately authorised members of the community, such as members of military associations or social and sporting clubs accessing Defence establishments.

5. DCACs and Defence issued identity cards are only to be issued to sponsored persons.

Example: *DCAC or Defence identity cards are not to be produced for Military Working Dogs or Unit mascots.*

6. Only DCACs supported by a record of positive identification (such as a passport or driver's licence) may be registered on EACS. Records that identify persons who have accessed specific Defence sites and/or assets, and when they were accessed, are required to be maintained and appropriately protected.

Note: *DCACs are to be deregistered from the EACS once they are no longer assigned to a positively identified individual or, in the case of Temporary Access DCAC, if they remain unaccounted for at muster (or 24 hours after issue).*

Note: *In accordance with Australian Privacy Principles this information must not be utilised for any other purpose and is to be protected from misuse, interference or loss.*

7. Visitors without DCAC or Defence issued identity cards are to provide alternative identification documents. These documents are to contain a recent photo and ought to be issued by an Australian Government entity, such as a current passport, or a licence or permit issued under a law of the Commonwealth, a State or Territory such as an Australian driver's licence.

Exclusion: *Minors may be positively identified by a parent or guardian who is the holder of a DCAC or Defence issued identity card, or has provided alternative identification documents as detailed above.*

Access Control Requirements

8. DSPF Principle 72 - *Physical Security* defines minimum standards for access to classified material and Physical Security Zones. These standards are to be met in order to maintain an area's security rating. Access to other areas and resources is determined through the security risk assessment process conducted by the local Commander/Manager or, with regard to whole-of-base access, the Base Support Manager (BSM) in consultation with Commanders and Managers.

Note: *Security risk assessments take into account the differences in local conditions that affect a base, establishment, facility, or military or business unit.*

Local Conditions of Access

9. The BSM and Senior ADF Officer (SADFO) jointly determine local conditions of access based on security requirements and workplace health and safety considerations. This ought to be done in consultation with resident Commanders and Managers.

10. It is recommended that such local arrangements are incorporated into base security documentation and are considered in SAFEBASE planning. Any local arrangements that may impact DCAC approval are to be broadly communicated across Defence. These access arrangements may be affected by changed circumstances at the site, such as the hosting of a major event or an increase in the SAFEBASE alert level.

Example: *Cleaning contractors are given a DCAC to allow them to conduct cleaning activities within a base. Normally they are permitted to enter the base unescorted to conduct their work. An increase in the SAFEBASE alert level may require them to be stopped at the gate and signed in as escorted visitors or be cleared to an appropriate level for unescorted access. Certain areas previously accessible for contracted cleaning may be off limits.*

Access Entitlement

11. Prior to granting authorisation for an individual seeking to gain unsupervised and unimpeded access to any part of a base (apart from a Zone 1 area), a Commander or Manager is to ensure that:

a. the individual has a legitimate need for access arising from:

   i. a performance agreement, a contract or a duty statement; or

   ii. a requirement or entitlement to access married accommodation or recreational facilities;

b. the proposed access is consistent with any local conditions of access determined by the BSM and SADFO;

c. if required, the individual holds an appropriate security clearance and any specific compartment briefing; and

d. the individual has a valid DCAC (except for minors under the age of 16).

Note: *A holder of a DCAC or Defence issued identity card is not automatically entitled to enter or access all areas within a Defence base, establishment, facility, or military or business unit.*

Contractor Unescorted Access

12. Contractors, Consultants and Outsourced Service Providers with unescorted access ought to have their access limited by making it time or circumstance specific. For example, in or out of business hours, only on weekdays or only weekends or during periods of heightened support to ADF operations. The responsibility for ensuring time or circumstance pre-requisite criteria for unescorted contractor access resides with the relevant Contract Manager.

13. Contractors, Consultants and Outsourced Service Providers who have not been granted an appropriate security clearance are required to be escorted at all times when accessing Zone 3 and above areas of a base.

Note: *Contractors, Consultants and Outsourced Service Providers do not need a security clearance if they only require access to controlled areas less than Zone 3, such as gardeners tending to grounds maintenance.*

Visitor Access

14. Any person not issued a personalised (and currently valid) DCAC is to be escorted by an appropriate DCAC holder at all times when accessing Controlled or Zone 2 and above areas of a base.

Access for Minors Under the Age of 16

15. Minors who are under 16 years of age, and therefore not entitled to hold a family member's DCAC or Defence issued identity card (refer Annex B of this Control - *Access and Identity Card Types*), are to be escorted at all times by a parent or legal guardian when accessing Controlled or Zone 2 and above areas of a base. However, the BSM of a base with on-site married accommodation may develop local arrangements allowing unescorted access to minors under the age of 16, where those minors are themselves residents of the base or are visiting residents of the base. It is recommended that in such circumstances unescorted access only applies to movements to, from and within married accommodation and community/recreational areas of the base. It is recommended that such local arrangements are incorporated into base security documentation and are considered in SAFEBASE planning.

Note: *The escorting of a minor under the age of 16 by a parent or legal guardian is considered to be a different circumstance to the 'formal' escorting of a visitor. Parents and guardians who hold a relevant family DCAC do not have 'formal' escorting rights (refer Annex B of this Control - Access and Identity Card Types for further information) for visitors, but are responsible for the movement of minors in their care.*

Issuing Identity and Access Cards

Unescorted Access Requirements

16. All applications for DCACs and Defence issued identity cards will identify a Defence sponsor who accepts the risk of the sponsored individual gaining unescorted access. It is recommended that a Security Officer (qualified and promulgated) within the relevant military or business unit be the Defence sponsor. The Defence sponsor:

a. is required to be either an ADF member or a Defence APS employee;

b. ought to at a minimum be at the APS6/04 level, unless the individual is in the position of Security Officer in the sponsoring business unit; and

c. should be in the business unit that has some functional or professional responsibility for or association with, the supervision of, or function/service being performed/facilitated by, the DCAC applicant or their employing organisation.

Exclusion: *Group Heads and Service Chiefs may, for areas of their sole responsibility, dictate if Defence sponsors are to be higher than APS6/O4 level. Commanders and Managers of Defence bases, where a Defence sponsor at the APS6/O4 level is not employed, may take on the role of the Defence sponsor.*

Note: *Security Officers' approval of Defence issued identity cards can differ depending on the card. For further advice refer to the National Pass Office (Estate and Infrastructure Group (E&IG)).*

17. With respect to sponsorship of family members:

a. ADF members may sponsor their own family members for the issue of mauve, or base-specific red with banding family (Uncleared) DCAC; and

b. APS employees may sponsor their own family members for the issue of red with banding family (Uncleared) DCAC limited to a specific base.

Note: *APS employees' family members are not entitled to the National Defence family (mauve). For further information on the specific cards refer Annex B of this Control - Access and Identity Card Types.*

18. Defence personnel sponsoring a family member are to accept responsibility and be accountable for the ongoing use of the card by their family member. The spouse/dependant (applicant) is required to present a printout from the sponsor's current PMKeyS record (Dependants page for ADF or Emergency contacts for APS) that confirms the applicant's relationship to the sponsor. The sponsor is not required to attend the pass office with the applicant.

Note: *The details on the PMKeyS printout are to match the applicant's positive identification documents (such as a driver's licence or passport). Neither the printout nor copies of these identification documents are to be retained by the pass office.*

19. DCAC or Defence issued identity cards will only be given to individuals by a pass issue officer upon presentation/completion of:

a. a suitable form of valid photographic, government or government agency issued identification document or card (such as a driver's licence or passport);

b. proof of a legitimate need for unescorted entry to the area (i.e. sponsorship) if applicable;

c. a signed and witnessed 'Conditions of Use' form;

d. where required, proof of a security clearance; and

e. if relating to a family member's card, proof of relationship to the sponsoring member.

20. DCAC and Defence issued identity cards are to include the holder's first name and surname, and a current photograph of the holder. The Conditions of Use of a DCAC and Entry to Defence Sites is acknowledged by the recipient's signature at the time of card issue.

21. Details of specific DCACs and the requirements associated are found in Annex B of this Control - *Access and Identity Card Types*.

22. Card issuing equipment and blank cards are to be kept secure at all times at the base, establishment, facility, or military or business unit which they service.

23. Before a DCAC for entry to a Defence facility is granted to a Contractor, Consultant or Outsourced Service Provider, the Defence sponsor is to provide an approved DCAC application form to the pass issue officer that confirms:

a. the requirement for access;

b. the areas where access is required;

c. the agreement of all affected Commanders and Managers (or their Security Officers), where access is required across multiple facilities if the applicant does not hold a security clearance; and

d. the validity period approved for the card (e.g., the end of the contract).

24. The red base specific DCAC (refer Annex B of this Control - *Access and Identity Card Types*) is the default card issued to all Contractors, Consultants and Outsourced Service Providers. If the sponsor has confirmed that the Contractor, Consultant or Outsourced Service Provider has an Australian security clearance and a legitimate need to regularly access other parts of the Defence estate across Australia then the provider may be approved for issue of a yellow Defence industry DCAC.

25. The sponsor is required to ensure that the expiry date for the DCAC of a Contractor, Consultant or Outsourced Service Provider does not extend beyond the date of contract expiry and is within the limits detailed in Annex B of this Control - *Access and Identity Card Types*.

Escorted Access Requirements

26. Where a visitor is issued a ‘To be escorted Visitor’ DCAC (white/red), the escort officer does not have to be an ADF member or APS employee; however, the escort officer is required to have escorting entitlements associated with their DCAC (refer Key Definitions). For further requirements regarding visitor access refer to Annex A of this Control - *Visitor Access Control*.

Short Term Contractor or Base Resident Guest Pass

27. A temporary identification pass may be issued locally to manage short term (between 24 hours and 14 days), unescorted site access by approved Contractors, Consultants, Outsourced Service Providers, or personal guests of personnel living in on-base accommodation (refer Annex B of this Control - *Access and Identity Card Types*).

Conditions of Use

28. Every person given a DCAC or Defence issued identity card is to only use the card for the purpose for which that particular card was issued; refer Annex B of this Control - *Access and Identity Card Types*.

Example: *ADF Reserve members using their purple ADF DCAC to gain access to Defence facilities in order to carry out their civilian employment, or for personal or special interests, is considered an unauthorised use of their ADF DCAC.*

29. The conditions of use of the card will be acknowledged by the holder, upon issue, through signature of a 'Conditions of Use' form and witnessed by a member of the pass office where the card was issued. The signed, original 'Conditions of Use' form is to remain at the pass office; the card holder may receive a copy.

30. All holders of DCAC and Defence issued identity cards should be reminded that the use of cards for other than official Defence purposes increases the threat of identity theft and fraud. It is relatively easy for information obtained from a DCAC and Defence issued identity card to be used for fraudulent purposes.

31. It is recommended that personnel only use their DCAC or Defence issued identity cards for official Defence purposes or for the provision of Government services. Other options are typically available, such as, a driver's licence, birth certificate and passport. Personnel are not to replicate or transfer a copy of their DCAC or Defence issued identity cards (physically or electronically) to any other organisations or individuals.

32. Breaches of the acknowledged 'Conditions of Use' for a card are to be reported as a security incident in accordance with DSPF Principle 77 - *Security Incidents and Investigations*. If an investigation is warranted, the holder's use of the card may be suspended until an investigation has been completed.

33. When in a Defence establishment, the DCAC is to be worn at all times, contingent upon safety requirements. Holders are responsible for wearing the DCAC in a prominent position above the waist and in front of their body. Furthermore, holders of DCAC should:

a. protect the DCAC from loss, theft, defacement or unauthorised use;

b. clearly display the DCAC for inspection when entering a Defence or DISP establishment;

c. show the DCAC on demand to any appropriate authority who, in the course of their duty, requires proof of identity;

d. not wear the DCAC outside Defence or DISP facilities;

e. not lend the DCAC to any other person;

f. surrender the DCAC to their Supervisor, Commander or Manager when separating from Defence, or from a Contractors, Consultants, or Outsourced Service Provider; and

g. surrender the DCAC to a Defence Security Guard, Security Officer, or nearest Defence pass office when it is damaged, cannot establish positive identification, expires or when the holder no longer needs access to the area/s for which it was issued.

34. Defence personnel, Contractors, Consultants and Outsourced Service Providers are to challenge any person not wearing a DCAC in areas controlled for security reasons. If the person cannot provide a card, security staff are to be notified immediately.

Replacement of Identity and Access Cards

35. Personnel may be given a replacement DCAC or Defence issued identity card at the discretion of the Commander or Manager. Appropriate documentary evidence is to be provided by the member to justify a card replacement. Circumstances under which a card may be replaced include:

a. lost or stolen card;

b. defacement, deterioration or inoperability of the card;

c. a beard is grown or removed;

d. physical appearance has been significantly altered, such as hair length or colour;

e. a change in name or rank occurs;

f. movement between permanent or reserve elements of the ADF; or

g. movement between Services.

Lost or Stolen Identity and Access Cards

36. The holder of a DCAC or Defence issued identity card is required to report loss or theft of the card at the earliest opportunity to the relevant E&IG pass authority and their security officer. The security officer in turn is to confirm that the relevant pass authority has been informed and is to treat the loss as a security incident and report it in accordance with DSPF Principle 77 - *Security Incidents and Investigations*. Defence personnel, Contractors, Consultants and Outsourced Service Providers are to make every effort to recover the card.

37. When reported, the issuing authority will invalidate the card and only issue a replacement after confirmation by the supervisor/sponsor of the Defence personnel, Contractors, Consultants or Outsourced Service Providers that this is appropriate.

Return of Identity and Access Cards

38. Defence personnel separating from the APS or ADF are required to surrender their DCAC or Defence issued identity card (including family member cards) to their Commander or Manager for return to the nearest pass office for cancelling. This is to be part of the routine exit administration for all Defence personnel.

39. Contractors, Consultants and Outsourced Service Providers are to surrender their DCAC or Defence issued identity card to their supervisor or contract manager for return to the nearest pass office within five working days, on cessation of their contract or when no longer required. This is to be part of the routine exit administration at the conclusion of a contract or access requirement.

Note: *Where applicable, exit administration shall include the return of family member cards.*

40. The receiving pass office will mark as returned, cancel and/or invalidate all cards returned or no longer authorised. The card will have its top right corner removed and the remainder is to be held by the pass office for one year before being destroyed by cutting it into small pieces or being shredded.

41. Defence issued identity cards and DCACs remain Commonwealth property. The failure to surrender a Defence issued identity card or DCAC when required may result in administrative action.

Standard Operating Procedures and Templates

42. National Pass Office Management can provide information relating to standard operating procedures on the issue, replacement and return of DCAC or Defence issued identity cards. Templates of cards specified in Annex B of this Control - *Access and Identity Card Types* are controlled by the Directorate of Base Security Operations, Estate Services Delivery, E&IG.

Roles and Responsibilities

Deputy Secretary Estate and Infrastructure Group (DEPSEC E&IG)

43. DEPSEC E&IG is responsible for:

a. access control arrangements at all Defence bases and facilities covered by E&IG base services contracts;

b. determining standards and templates for DCAC, Defence issued identity cards and access control systems;

c. producing and distributing DCAC and Defence issued identity cards; and

d. instituting and maintaining a system that allows the loss or theft of a DCAC and Defence issued identity card to be reported by a Defence card holder at any time, alerts appropriate security staff of the loss and, if possible and necessary, blocks the lost or stolen card's access privileges.

Base Support Manager (BSM) and Senior ADF Officer (SADFO)

44. The BSM in consultation with SADFO and resident Commanders and Managers, is responsible for establishing access control measures in accordance with the Physical Security Zone methodology (refer to DSPF Principle 72 - *Physical Security*), at a whole-of-base level, and has the authority to:

a. grant, refuse or withdraw permission for Contractors, Consultants, Outsourced Service Providers, visitors and family members of Defence personnel to access bases, establishments, facilities, and military or business units on security grounds;

b. require pre-approval for access to specified areas outside of normal operational hours; and

c. determine any base-specific policy, additional or complementary to this DSPF part, under which unescorted access will be granted to an area, including setting any conditions such as access outside normal operational hours.

Note: *Any base-specific access control policy arrangements that may affect what is approvable by DCAC approval authorities, are to be communicated to the whole of Defence by the relevant BSM, through appropriate channels, to ensure associated DCAC application rejections are avoided.*

45. The BSM may advise Commanders and Managers where there has been a failure to comply with a reasonable and lawful direction in relation to APS employees, or a lawful order in relation to ADF members, which impacts on security. The matter may then be the subject of APS Code of Conduct or disciplinary action by the relevant authorities.

46. Generally SADFO assumes command of the relevant base in the case of a security, safety or emergency event requiring coordination of base personnel or resources. For the purposes of access control and identity management, SADFO assumes the responsibilities and authority of BSM, as detailed above, at the heightened SAFEBASE alert levels of DELTA and ECHO. For further information refer to DSPF Principle 83 - *SAFEBASE*.

Commanders and Managers

47. Commanders and Managers are responsible for:

a. implementing and ensuring compliance with appropriate access control measures in accordance with the Physical Security Zone methodology (refer to DSPF Principle 72 - *Physical Security*), for their organisation;

b. ensuring records of out-of-hours access by personnel to security containers or Physical Security Zones of level 3 or above are maintained, for example through the use of an EACS or a log book; and

c. if a local EACS is maintained, appointing an individual (generally a Security Officer), to undertake system administration activities, maintain oversight of its records and make them available for inspection in response to a security incident or investigation.

Note: *For further information on security incidents and investigations refer DSPF Principle 77 - Security Incidents and Investigations.*

Note: *The term 'Commanders and Managers', which is used throughout the Protective Security Policy Framework (PSPF), is interchangeable with the term 'Heads of Resident Units', used under the Base Accountability Model.*

48. Commanders and Managers have the authority to:

a. grant, refuse or withdraw permission for visitors, Contractors, Consultants or Outsourced Service Providers or family members of Defence personnel to access military or business units on security grounds;

b. limit or manage Defence personnel access to bases, establishments, facilities, and military of business units on security grounds;

Note: *Security grounds include changes to access and need-to-know brought about by changes to contracts, roles and postings. They may also include the requirement to limit access for disciplinary, conduct or performance reasons through suspension of duty.*

c. require pre-approval for access to specified areas within their unit lines outside normal operational hours; and

d. determine any military or business unit-specific policy, additional or complementary to this DSPF part, under which unescorted access will be granted within the military or business unit, including setting any conditions such as access outside of normal operational hours.

Security Officers

49. Security Officers assist Commanders and Managers of military or business units to fulfil their security responsibilities. This may include ensuring that a person who does not meet the criteria for unsupervised and unimpeded access is either denied access, or treated as a visitor by being recorded in the visitor register and accompanied at all times by an escort officer.

50. Security Officers (trained, appointed to and promulgated into the position), within the relevant military or business unit responsible, at any ranks/APS levels, may be delegated by Commanders or Managers to sponsor DCACs and, when appropriate, Defence issued identity cards.

Contract Managers

51. Contract Managers (APS/ADF) are responsible for:

a. consulting with the relevant BSM regarding:

   i. the contractor's required level of access to Defence facilities; and

   ii. any out of hours or escorting privileges to be associated with DCACs held by Contractors, Consultants or Outsourced Service Providers without a security clearance, for access to those facilities; and

b. ensuring the return of DCACs and withdrawal of access to Defence facilities when a contract has ended or Contractors, Consultants or Outsourced Service Providers no longer have an access requirement.

Defence Personnel, Contractors, Consultants and Outsourced Service Providers

52. Defence personnel, Contractors, Consultants and Outsourced Service Providers are responsible for:

a. accessing only those areas and systems to which they have been authorised;

b. complying with the terms and conditions of DCAC use, including wearing their DCAC at all times, in a prominent position when in a Defence establishment;

c. promptly reporting the loss or theft of their (or a family member's) DCAC or Defence issued identity cards; and

d. returning their (and any family member's) DCAC and Defence issued identity cards when separating from the APS or ADF, or for Contractors, Consultants and Outsourced Service Providers at the conclusion of a contract unless other arrangements have been made with the Defence access sponsor.

Key Definitions

53. **Access Control**. The ability to control access to designated areas, information or other assets requiring protection.

54. **Controlled Area**. An area that is inside a Defence-established or base perimeter with controlled access, but which is outside of a Physical Security Zone 3 or higher. Persons not previously issued a personalised (and currently valid) DCAC are to be escorted by an appropriate DCAC holder in these areas.

55. **Escort Officer**. An individual charged with the responsibility of supervising the movements of a visitor to a designated area. Only an individual identified by their DCAC (detailed in Annex B of this Control - *Access and Identity Card Types*) as having escorting entitlements may perform the role of an escort officer.

56. **Unescorted Access**. A type of access granted to an individual who has been positively identified, holds an appropriate security clearance, has a confirmed need to access an area and has been authorised to do so.

57. **Identity Card**. A card used for identification purposes. It identifies an individual, but does not grant access to any assets or information.

58. **Access Card**. A card that grants access to Defence assets and information. It may contain an electronic access token, which permits automated entry to an area, or access to an ICT system.

59. **Defence Common Access Card**. An access and identity card, which may also be programmed for use on an EACS, for those establishments and facilities which the holder has a legitimate need to access in performance of their duties.

60. **Family Member**. An individual who is considered a 'dependant' of an Australian Defence Force (ADF) member or an APS employee. The term ‘dependant’ is defined in:

a. the Pay and Conditions Manual (PACMAN) for ADF members; and

b. the Defence Enterprise Agreement (DEA) for APS members.

Further Definitions

61. Further definitions for common PSPF terms can be found in the Glossary.

62. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – *Visitor Access Control*

Annex B – *Access and Identity Card Types*

Document Administration

Identification

DSPF Control	Access Control
Control Owner	DG ESD
DSPF Number	Control 74.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Access Control
Related DSPF Control(s)	Classification and Protection of Official Information Defence Industry Security Program Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Personnel Security Clearance Physical Security Identification, Search and Seizure Regime 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	DG ESD	Launch

Defence Security Principles Framework (DSPF)

Annex A to Access Control – Visitor Access Control

Advance Notification of Clearances

1. When Defence personnel, Contractors, Consultants and Outsourced Service Providers visit another Defence base, or Defence industry facility, where a Defence Common Access Card (DCAC) or pass is required for entry, or there is a need to discuss classified information, the point of contact (usually the Visit Host) is to notify the host's Security Officer to confirm the Visitor's security clearance level and briefings, before entry. The Security Officer can confirm the currency on the Personnel Security Assessment Management System, or with the Defence Security and Vetting Service (DS&VS).

Process for Visitor Access to Defence Establishments

2. The process outlined in the table below is to be followed for all Visitors to Defence establishments.

Table 1 – Process for Visitor Access to Defence Establishments

Step	Who does it	Action
1	**Visit Host**	Provides advance notification of Visitor details to the Guard or Receptionist, including name and expected time of visit,.
2	**Visitor**	Communicates to the Guard or Receptionist the purpose of their visit and the name of their Visit Host.
3	**Guard or Receptionist**	a. telephones the Visit Host to confirm the Visitor is expected and has arrived; b. positively identifies the Visitor; and c. issues the Visitor with a Visitor DCAC and advises they are to wear it at all times while on the premises.
4	**Visitor**	At all times: a. displays their Visitor's DCAC in a prominent position; and b. remains with their Visit Host.

Step	Who does it	Action
5	**Visit Host**	a. authorises access for the Visitor and signs the Visitor register (which includes details such as the Visitor's name, the Visitor's agency/firm or private address, name of individual/area to be visited, the reason for the visit, and the arrival and departure times); b. provides the Visitor with a base induction briefing including emergency response arrangements and other relevant security considerations (eg. security searches); c. escorts the Visitor throughout the visit; d. ensures that the Visitor does not gain unauthorised access to classified information or capabilities; e. escorts the Visitor to the exit; and f. confirms the Visitor has left the site and returns the Visitor's DCAC to the Guard or Receptionist at the end of the visit.
6	**Guard or Receptionist**	Within 24 hours of Visitor DCAC issue: a. ensures that all Visitor passes have been returned, and accounts for any Visitor passes yet to be returned; and b. on return, disable Visitor passes that give access to any access control systems.

Media Representatives

3. Commanders and Managers are to consult with Communication and Public Affairs, or their authorised representative, to confirm whether permission to enter a Defence establishment can be granted to media representatives and on what conditions. Specific guidelines are found in the Defence Communication Manual, Chapter Two, Media engagement and public comment.

4. In addition to the requirements of paragraph three and the process outlined in Table 1 above, it is recommended that the following procedures be applied:

a. prior to giving the media representative access to a Defence establishment, the DS&VS regional office is consulted;

b. an Escorting Officer is assigned to accompany the media representative throughout the visit;

c. security classified information is secured or, as a minimum, protected from view throughout the visit; and

d. when appropriate, additional restrictions are considered, such as handing in mobile phones and other recording and communications equipment.

5. If access is granted to areas where classified resources are being used or handled, the Escorting Officer is to remind the media representative that no photographs or recordings of any type can be taken at any time during the visit.

Officials with Statutory Rights to Enter Workplaces

6. The processes outlined in Table 1 above for controlling visitor access and escorting visitors are to be applied during the visit of officials who have a statutory right to enter workplaces (e.g. trade union and Comcare officials). Visiting officials may enter only for purposes related to their role under relevant legislation, such as under the *Fair Work Act 2009* or the *Work Health and Safety Act 2011*.

Parliamentarians and Candidates for Election to Parliament

7. The Minister for Defence is required to be informed of any proposed visit to Defence establishments by Parliamentarians and candidates for election, and will approve access by such persons if access to security classified resources or entry to secure areas is required. Further information will be provided by the Ministerial and Parliamentary Branch.

Foreign Nationals on Official Travel

8. Commanders and Managers are responsible for:

a. ensuring that areas containing security classified resources are protected from observation or excluded from any tour of inspection by foreign nationals on official travel. Security classified resources are to be screened and covered in their entirety, so as to give no indication of their purpose or scope. Similar procedures are to be followed in relation to tallies, name tags/plates and cables, which would identify security classified resources; and

b. appointing and briefing the Escorting Officer to accompany the foreign national/s throughout the visit. The Escorting Officer is required to be briefed on the unit specific security requirements for foreign nationals.

9. Hosts and sponsors of foreign nationals are responsible for abiding by DSPF Principle 15 - *Foreign Release of Official Information*.

10. If confirmation of the foreign nationals security clearance details is required, this can be arranged by ensuring they request their details are forwarded to the DS&VS International Visits Office.

11. If foreign release of official information is being risk managed under DSPF Principle 15 - *Foreign Release of Official Information* the DCAC sponsor will need to consider access arrangements.

Note: a Foreign National cleared DCAC (green) *is not to be issued to foreign personnel without a recognised clearance.*

Foreign National on Unofficial Travel

12. In the highly unusual circumstance of a request by a foreign national on unofficial travel to visit a Defence or Defence Industry establishment, they are to be treated as a visitor and escorted at all times as outlined in Table 1 above. The Visit Host will report their visit details to the DS&VS International Visits Office. Knowledge of the person and their status within their own country is not sufficient for the Visit Host to permit access.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Visitor Access Control
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control)
DSPF Control	Access Control
DSPF Number	Control 74.1

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	DG ESD	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B to Access Control – Access and Identity Card Types

Defence Common Access Cards – General Access

1. The following Defence Common Access Cards (DCAC) entitles the holder to unescorted access to facilities for which they have the appropriate security clearance, and a legitimate need to access. DCAC types are differentiated by a combination of colours and attributes (e.g. banding). Dependent upon the date of issue, the DCAC may contain an additional text-based identifier of the card's colour.

Note: *A DCAC is an identity and access card suitable for identifying personnel at all Defence facilities, and which may be programmed for use on an Electronic Access Control System (EACS) for those facilities, which the holder has a legitimate need to access in the performance of their duties.*

2. In all cases foreign nationals may only be issued a Foreign National DCAC (green) (cleared or uncleared dependent on the circumstances), or a Temporary Access Pass (subject to any Australian citizen requirements).

Exception: *Foreign national personnel as described at paragraph 4c below, or recognised family members of Australian Defence Force (ADF) members or Defence Australian Public Service (APS) employees.*

3. **Australian Defence Force DCAC (Purple).** To meet Article 17 of the Third Geneva Convention of 1949, the ADF DCAC must include:

a. the holder's first name and surname;

b. the holder's rank, Service number, and date of birth; and

c. the conditions of issue.

4. The purple ADF DCAC is to be issued to:

a. permanent members of the ADF on arrival at initial training or posting;

b. Working Reserve personnel rendering continuous full time service ;

Note: *Working Reserve personnel issued the purple ADF DCAC retain the card for the duration of their formal ADF engagement or until the card expires. Standby Reserve (SERCAT 2) members are ineligible to receive this DCAC as they do not render service and have no service obligation.*

Note: *Working Reserves are reminded that the purple ADF DCAC is only to be used for the purpose for which the card was issued, i.e. Working Reserve or continuous full time service.*

c. Former members of the armed forces of the UK, US, Canada, NZ or other countries who have enlisted or been appointed into the ADF under the government to government 'ADF lateral recruit' program, and whose Australian citizenship is pending. See DSPF Principe 40 - *Personnel Security Clearance Process* for further details;

d. authorised philanthropic staff working with ADF units (e.g. Salvation Army), when required; and

e. permanent staff (civilian) employed by the ADF in an area of operation (AO) for the duration of that employment. This card is to be used as an identification document for easy recognition by allied forces to facilitate appropriate access rights. It does not replace the Geneva Convention card which is issued separately under the direction of Chief Joint Operations (CJOPS). This card is not to be used outside the AO and is to be returned to the issuing office upon return.

Exception: *Recruit/trainee DCAC (orange). This card may be issued to recruits or trainees on arrival at initial training, as an alternative to the purple ADF DCAC. Adoption of this exception will be determined by the resident Base Support Manager (BSM) and Senior ADF Officer (SADFO) after consultation with the respective Service or Group Security Adviser. This DCAC expires upon completion of initial training and is to be returned to the place of issue for cancellation. This card is normally base-specific, however a maximum of eight bases/facilities may be approved. Additional restrictions may be imposed at the relevant Commander's discretion.*

5. The purple ADF DCAC is not base specific and gives the holder after hours and escorting privileges. This DCAC will have a maximum expiry date of five years from the date of issue, which is printed on the front of the card. This is to allow the purple ADF DCAC to be used as a form of identity for Centrelink and other Government services (Centrelink require expiry dates on all forms of identity).

6. **Defence Australian Public Service (APS) DCAC (Blue).** Issued upon appointment to permanent civilians employed by Defence. The blue APS DCAC gives the holder after hours and escorting privileges to facilities where they have the appropriate security clearance, and a legitimate need to access. This DCAC will have a maximum expiry date of five years from the date of issue, which is printed on the front of the card. This DCAC is not base specific.

7. Non-ongoing civilians employed by Defence are issued the blue APS DCAC; however it is required to be annotated with the term 'non-ongoing staff'. The DCAC is to expire and be returned upon completion of the employment contract.

8. **Defence Industry/Agency DCAC (Yellow).** Issued to Contractors, Consultants and Outsourced Service Providers who support Defence and who require regular access to Defence sites nationally. These persons are required to have a minimum BASELINE security clearance.

9. Contractors, Consultants and Outsourced Service Providers require the relevant ADF/APS contract manager's (or authorised delegate in the business unit) approval to be issued this card. Contractors, Consultants and Outsourced Service Providers eligible for this DCAC type include, but are not limited to:

a. employees of a company contracted to Defence, (Defence Industry Security Program (DISP) and non-DISP);

b. individual contractors contracted to Defence (DISP and non-DISP);

c. external agency staff (staff of Non-corporate Commonwealth entities as stipulated under the *Public Governance, Performance and Accountability Act 2013* (PGPA) and summarised in the Flipchart of Commonwealth entities and companies); or

d. employees, contractors or subcontractors of the Army and Air Force Canteen Service (AAFCANS), trading as Frontline Defence services, commonly known as Frontline.

Note: *AAFCANS differs from other companies contracted to Defence as they are a Corporate Commonwealth Entity established by Regulation in accordance with the Public Governance, Performance and Accountability Act 2013 (PGPA). AAFCANS is governed by the Army and Air Force (Canteen) Regulations 2016 via the Defence Act 1903 to provide amenities services for Defence. Requests for Defence industry/agency cards associated with AAFCANS/Frontline are to be made through their head office to the Directorate Forces Entertainment and ADF Support Services.*

10. The Defence industry/agency DCAC may be approved and issued following confirmation of the individual's minimum BASELINE security clearance, and relevant contract commencement. The card is required to have an expiry date printed on the front. The expiry date is to be the lesser of:

a. the last day of the holder's requirement to hold the DCAC under the relevant contract; or

b. three years from the date of issue of that DCAC.

Note: *The sponsor may, at their discretion, specify an earlier date for expiry of the DCAC.*

11. National after hours and escorting privileges for this DCAC is only to be granted after approval has been given by the sponsor with full justification provided.

12. **Air Base DCAC (Yellow).** Issued to authorised Airservices Australia Flight Inspection Services personnel, for air base access from air side and road side to all Royal Australian Air Force air bases, Oakey and HMAS ALBATROSS. The yellow air base card is to be returned upon expiry or cancellation of the holder's Aviation Security Identification Card, or cessation of employment in flight inspection duties. The card will have a maximum expiry date of 12 months from the date of issue, which is printed on the front of the card.

13. **National Defence Family DCAC (Mauve).** Issued upon application, to recognised family members aged sixteen years and older of ADF permanent and Working Reserve members. The mauve family DCAC is not base specific and allows the holder to access domestic base married accommodation and family/community areas only. There is no requirement for the family member to hold a security clearance and there are no escorting privileges associated with this card.

Exception: *Mauve DCAC holders, 18 years of age and older, living in on-base married quarter residences within base perimeter access control points, may be approved escorting privileges, but only for the base on which the holder resides.*

Note: *Even though mauve family DCAC holders do not have any 'formal' escorting privileges, they are still responsible for escorting any minors under the age of 16 in their care.*

14. The mauve family DCAC will have a maximum expiry date of three years from the date of issue, which is printed on the front of the card. Sponsoring ADF members are to ensure that cards are renewed when required or returned when there is no further entitlement. If a family member is denied the issue of a mauve family DCAC or has their DCAC revoked, then they may be, at the discretion of the relevant base Commander or Manager, approved a red base access only DCAC (see below).

Defence Common Access Cards – Limited Access

15. The following DCAC are limited for access to specific bases/facilities only. They may be authorised for use on more than one base (e.g., those that are geographically close, within an Australian State or Territory), but this is subject to a documented regional agreement between relevant BSMs. Holders are not entitled to unescorted access to areas other than those approved for uncontrolled public access unless otherwise stated in the details of the specific DCACs below.

Note: *Unescorted access may be granted by the approval authority if a valid Australian security clearance is held.*

16. **Limited Base Cleared DCAC (Red).** Issued to authorised persons, holding a minimum BASELINE security clearance, determined eligible for permanent or periodic access to up to eight specified bases/facilities, or up to three States or Territories by the DCAC sponsor or approval authority. The card is to have an expiry date printed on the front. The expiry date will be the lesser of:

a. The last day of the holder's requirement to hold the DCAC under a relevant contract; or

b. Three years from the date of issue of that DCAC.

Note: *The sponsor may, at their discretion, specify an earlier date for expiry of the DCAC.*

17. Holders of the Limited base cleared DCAC (red) can include:

a. Contractors, Consultants and Outsourced Service Providers who are Australian citizens, have a minimum BASELINE security clearance and are working at the particular facilities for which the card is issued. The card will be annotated by the term 'Industry' or 'Contractor/PSP'; and

b. AAFCANS/Frontline employees, contractors or subcontractors who are Australian citizens, have a minimum BASELINE security clearance and are working at the particular facilities for which the card is issued. The card will be annotated by the term 'AAFCANS'.

18. **Limited Base Uncleared DCAC (Red with Banding).** Issued to individuals that are Australian citizens that do not hold an Australian security clearance, to access up to eight bases/facilities or a single State or Territory.

19. This card is issued upon contract commencement, as approved by the sponsor or as directed by the relevant approval authority (or authorised delegate, e.g. Security Officer). The card is required to have an expiry date printed on the front. The expiry date will be the lesser of:

a. The last day of the holder's requirement to hold the DCAC under a relevant contract; or

b. 12 months from the date of issue of that DCAC.

Note: *The sponsor may, at their discretion, specify an earlier date for expiry of the DCAC.*

20. Holders of the Limited base uncleared DCAC (red with banding) can include:

a. recognised family members aged 16 years and older, of APS employees posted both domestically or overseas. The red with banding family DCAC shall be annotated by the term 'Family' and is limited to one base only;

Note: *Non-Australian citizen family members of APS employees are also entitled to this DCAC.*

b. recognised family members aged 16 years and older, of ADF personnel in possession of an ADF (purple) DCAC (also refer paragraph 13 above). The red with banding family DCAC shall be annotated by the term 'Family' and is limited to one base only;

Note: *Family members of who remain in residence while the Defence member is posted elsewhere may retain their red with banding DCAC for that base until such time that they move to a new locale or are issued the mauve DCAC.*

Note: *Holders of red with banding DCACs annotated by the term 'Family' do not have any 'formal' escorting privileges, however they are still responsible for escorting any minors under the age of 16 years in their care.*

c. personnel authorised only to access community areas on a base, such as the golf club, gym, pool, or mess, who may be approved the red with banding DCAC annotated with the term 'Community Areas Only'; and

d. employees of Contractors, Consultants and Outsourced Service Providers and staff with no security clearances who may be approved the red with banding DCAC annotated with the term 'Uncleared' or 'Delivery Uncleared'.

Note: *Contracted employees and Community Areas Only DCAC applicants who are non-Australian citizens without a Defence recognised security clearance (other than those entitled to a National Defence family DCAC (mauve)) are to be sponsored for and issued the Foreign National 'Uncleared' green with banding DCAC.*

21. The red with banding DCAC is to be returned upon expiry of the contract or posting, cessation of dependency, or as directed by the DCAC sponsor, Commander or Manager (or their authorised delegate).

22. Escorting and after hours privileges for the red with banding DCAC will only be granted with the approval of the sponsor and with full justification provided.

Exclusion: *Contractors, Consultants and Outsourced Service Providers who do not have a security clearance may, under local arrangements at the discretion of the BSM/SADFO, be granted escorting or after hours privileges for the purpose of their employment on the base and with respect to those parts of the base to which they have access. In such circumstances the word 'ESCORT' and/or 'AFTER HOURS' is to be printed on the back of their red with banding DCAC and it is recommended that such local arrangements are incorporated into base security documentation and are considered in SAFEBASE planning.*

ADF Cadet DCAC

23. **Australian Defence Force Cadets DCAC (Grey).** ADF Cadet members are to be issued with a grey ADF Cadet DCAC upon appointment or enrolment in the Australian Navy Cadets (ANC), Australian Army Cadets or the Australian Air Force Cadets (AAFC). ADF cadet DCAC are to be issued using the same requirements as all other DCAC and Defence issued identity cards. This card is normally base specific, however a maximum of eight bases/facilities may be approved.

Note: *There is no requirement for a person issued this DCAC to hold a security clearance.*

24. The grey ADF Cadet DCAC is issued to:

a. cadets for a maximum of three years;

b. registered volunteers for a maximum of 12 months;

c. adult staff (officers and instructors of cadets) for periods not exceeding the length of their instrument of appointment or a maximum of five years, whichever is the lesser; and

d. parents and legal guardians of cadets for a maximum of three years, to allow them to transport their child to and from a cadet unit within a Defence base, where authorised by the BSM.

Note: *Grey ADF Cadet DCAC for the parents and guardians of cadets are to be base access only with the name of the base/s clearly annotated on the front*

25. The grey ADF Cadet DCAC will only be used for the purposes of official cadet activities. The card entitles the holder to unescorted access to facilities for which they have the appropriate security clearance and a legitimate need to access (i.e. official cadet activities). Holders of a grey ADF Cadet DCAC who are also ADF or APS members are not to use any other DCAC when acting in their cadet or cadet-related capacity to gain higher access to other areas.

26. Local access control arrangements between ADF Cadets and relevant BSM are to be negotiated where a cadet unit is located on a Defence base or facility. It is recommended that such local arrangements are incorporated into base security documentation and are considered in SAFEBASE planning.

27. Only adult staff have escorting privileges for the purposes of official cadet activities on a Defence base or facility. In such circumstances the word 'ESCORT' is to be printed on the back of their grey ADF Cadet DCAC. Cadets, registered volunteers and parents/legal guardians are not to be given escorting privileges on a Defence base or facility. The BSM may decide where and under what circumstances escorting may take place on their base or facility.

Foreign National DCAC

28. The cleared and uncleared Foreign National DCAC are issued upon contract commencement, posting or as directed by the Commander or Manager. The DCAC is to have an expiry date of 12 months from the date of issue, which is printed on the front of the card. The DCAC is to be surrendered:

a. upon expiry, completion of contract or posting;

b. if the holder ceases employment with the company they represent;

c. if the holder becomes an Australian citizen;

d. if the holder returns to their country of origin; or

e. as directed by the Commander or Manager.

Exclusion: *Holders of a Foreign National DCAC may (under strict conditions) be granted after hours and/or escorting privileges for the purpose of their employment on the base and with respect to those parts of the base where they have access. Refer to the paragraphs below for additional information on Foreign National cleared and uncleared DCAC.*

29. Foreign National Cleared DCAC (Green). Issued to non-Australian citizens who have a Defence recognised security clearance in accordance with DSPF Principle 15 - *Foreign Release of Official Information*. The holder must require regular unescorted access to bases/facilities requested upon application for this DCAC.

30. This DCAC may be issued to allow access to:

a. a specific Defence base/facility (up to eight may be specified);

b. bases/facilities within a State or Territory (up to three States or Territories may be specified); or

c. (under limited circumstances) national access.

Note: *The holder of a national access (green) DCAC may still require an escort or be prohibited access by local access requirements in force at any base/facility.*

31. Sponsors of this DCAC are responsible for:

a. ensuring that the Defence Security and Vetting Service International Visits Office has issued a Defence Security Advisory Visits notification (DSAV) number prior to application for this DCAC; and

b. confirming that the holder has legitimate access requirements for regular unescorted access to bases/facilities requested upon application for this DCAC.

32. Under local arrangements and strict conditions imposed by the BSM/SADFO, holders may be granted after hours and/or escorting privileges with respect to those parts of the specific bases to which they have access. In such circumstances the word 'ESCORT' and/or AFTER HOURS is to be printed on the back of the DCAC. It is recommended that such local arrangements are incorporated into base security documentation and are considered in SAFEBASE planning. Sponsors may request these privileges, with full justification provided, however final approval from the BSM will only be granted in exceptional circumstances.

33. Individuals eligible to hold a Foreign National cleared DCAC (green) may include, but are not limited to:

a. foreign employees of companies contracted to, or engaged by Defence;

b. officials of foreign government departments, agencies or authorities;

c. foreign military staff on long-term posting to Australia; and

d. foreign forces' personnel on the strength of a foreign Defence force unit lodged on an ADF base, or foreign forces' personnel who are training with, or temporarily attached to, the ADF. This card shall be annotated with the term 'Foreign Military Detachment' and is to be returned upon completion of detachment.

Exclusion: *Former members of the foreign armed forces who have enlisted into the ADF under the government to government 'ADF lateral recruit' program and whose Australian citizenship is pending are entitled to the purple ADF DCAC. They are not to be issued a green DCAC.*

34. **Foreign National Uncleared DCAC (Green with Banding).** Issued to non-Australian citizens that do not hold a Defence recognised security clearance. This DCAC allows access to up to eight bases/facilities or a single State or Territory. The holder requires a legitimate requirement for regular unescorted access to:

a. a number of Defence establishments; or

b. a facility(s) within a single Defence establishment.

35. Individuals eligible to hold a Foreign National uncleared DCAC (green with banding) may include, but are not limited to:

a. foreign employees of Contractors, Consultants and Outsourced Service Providers engaged by Defence;

b. non-Australian citizen dependants of holders of Foreign National cleared DCAC (green) on long-term engagements or postings to Defence units;

c. officials of foreign government departments, agencies or authorities;

d. foreign military staff on long-term posting to Australia;

e. foreign forces' personnel on strength at a foreign Defence force unit lodged on an ADF base, or foreign forces' personnel who are training with, or temporarily attached to, the ADF. This card shall be annotated with the term 'Foreign Military Detachment' and is to be returned upon completion of detachment; and

f. members of the public requiring base community areas only access.

Note: *Under local arrangements and strict conditions imposed by the BSM/SADFO, holders may be granted after hours and/or escorting privileges with respect to those parts of the specific bases to which they have access. In such circumstances the word 'ESCORT' and/or AFTER HOURS is to be printed on the back of the DCAC. It is recommended that such local arrangements are incorporated into base security documentation and are considered in SAFEBASE planning. Sponsors may request these privileges, with full justification provided, however final approval from the BSM will only be granted in exceptional circumstances.*

Identity Cards – No Access

36. There are no unescorted base/facility access or escorting privileges associated with the Defence issued identity cards detailed below. These cards are used for proof of identity only.

37. **Geneva Convention Card (White).** This card is issued to non-military staff working in operational areas under the direction of CJOPS.

38. **Standby Reserve Card (Grey).** Issued to all personnel transferring from the Permanent or Active Reserve forces to the Standby Reserve. The card has a maximum expiry date of five years from the date of issue, which is printed on the front of the card. Cards may be renewed subject to the member meeting individual Service requirements.

Note: *Working Reserve personnel undertaking continuous full time service are entitled to exchange the Standby Reserve card for a purple ADF DCAC upon commencement of the period of continuous full time service (or relevant contract).*

39. **Retired Member Card (Grey).** Issued to all members separating from the ADF who have a Level 3 entitlement under the Career Transition Assistance Scheme provisions contained in the ADF Pay and Conditions Manual. Level 3 is defined as 18 years or more service, or has left the ADF compulsorily for any of the following reasons:

a. medically unfit to continue service;

b. compulsory retirement age;

c. management-initiated early retirement; or

d. to meet the needs of the Service (i.e. declared redundant).

40. The entitlement to a retired member card does not apply to a member whose service is terminated on disciplinary or adverse administrative grounds.

Temporary Access

41. **Unescorted pass Positive Identity (White/Green).** The Positive Identity pass is only to be issued at base perimeter access points to Australian citizens with a Defence recognised security clearance, and is to expire after one day and be returned to the place of issue. Holders of the pass do not need to be escorted. There are no after hours or escorting privileges associated with this pass. These passes may be enrolled on unit Electronic Access Control Systems, but for no longer than 24 hours, and only for the individual to whom the pass is issued. These passes are not to be taken off-base and will be mustered by the issuing office within 24 hours of issue.

42. This pass may be issued to authorised personnel:

a. holding a current Limited Access DCAC but who do not have day to day access rights to the facility or base being visited; or

b. who have been provided with a Defence issued identity card or DCAC but do not have their card in their possession (for example the card has been lost or left at home).

43. **To Be Escorted Visitor DCAC (White/Red).** This DCAC type is to expire 36 months after the date of production. This DCAC is only to be issued at base perimeter access points. Holders of this DCAC are required to be escorted. This DCAC is base specific and is to be returned within 24 hours of the time of issue, to the place of issue. These DCAC types are not to be taken off-base and will be mustered by the issuing office within 24 hours of issue.

44. This pass may be issued to authorised visitors to a Defence base including:

a. media representatives;

b. contractors;

c. members of the public;

d. parliamentarians and candidates for election to Parliament;

e. foreign nationals on official or unofficial travel; or

f. trade union and Comcare officials.

45. **Very Important Person (VIP) Pass (White).** Issued to two-star ranked (and civilian equivalent) officers and above on a 'needs basis', being:

a. in the event of a visit to a Defence base or facility; or

b. to facilitate access for spouses, partners and guests of three-star ranked (and civilian equivalent) officers and above.

46. VIP DCAC are to expire 12 months after the date of production and are only be issued at base perimeter access points. These DCAC may be issued for the date of the VIP visit, are not to be taken off-base and will be mustered by the issuing office within 24 hours of issue.

47. Holders of this pass are to be escorted.

48. **Short-term Contractor or Guest Pass.** A temporary identification pass which may be produced by a local site pass/visitor management system. The pass is subject to BSM/SADFO approved local arrangements and is for the purposes of:

a. managing short term site unescorted access by approved contractors; or

b. providing short term (between 24 hours and 14 days), unescorted site access for personal guests of personnel living in on-base accommodation.

49. These passes are to clearly display:

a. the specific base to which they apply;

b. the area within the base to which access has been granted; and

c. the expiry date for that access.

Note: *The expiry date is to reflect the term of the contract or the period of the guest's visit, up to a maximum of 14 days.*

50. The pass must also display the holder’s photograph, full name and (if a contractor), the company for whom they work. In the case of guests, their host’s full name is also to be included.

Note: *Photographs are to be of a size and quality equivalent to those printed on an issued DCAC. It is not sufficient to copy any part of an existing identification for this purpose.*

Note: *Personnel living in on-base accommodation hosting an approved visiting guest, remain responsible for their guest while on the base being visited.*

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Access and Identity Card Types
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Access Control
DSPF Number	Control 74.1

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	DG ESD	Launch

Defence Security Principles Framework (DSPF)

Contracted Security Guards

General principle

1. Contracted security guards contribute to the protection of:

a. Defence assets and infrastructure from theft or damage; and

b. official information, facilities, information and communication technology (ICT) systems from unauthorised access.

Rationale

2. Contracted security guards are an element of an integrated security system to detect, deter, deny, and (in a limited capcity) respond to security threats and incidents at Defence bases and facilities.

3. Guarding requirements are based on the assessed needs for the security of personnel, information and physical assets at the base or facility.

Expected outcomes

4. Defence maintains an efficient, effective and credible contracted guarding service.

5. Contracted security guards engaged by Defence are:

a. trustworthy;

b. qualified;

c. appropriately licensed/accredited; and

d. properly briefed/instructed with regard to their duties.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager.
Moderate	EL2 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations.
Significant	Director General Estate Service Delivery (DG ESD).
High	Defence Security Committee (DSC) – through First Assistant Secretary Service Delivery (FAS SD).
Extreme	Defence Security Committee (DSC) – through FAS SD.

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Contracted Security Guards
Principle Owner	First Assistant Secretary Security and Vetting Services (FAS DS&VS)
DSPF Number	Principle 75
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 75.1
Control Owner	DG ESD

Related information

Government Compliance	**PSPF Core Requirements**: Entity physical resources and Entity facilities **Legislation**: *Work Health and Safety Act 2011 (Cth)* *Privacy Act 1988 (Cth)* *Security Industry Act 2003 (ACT)* *Security Industry Act 1997 (NSW)* *Private Security Act 1995 (NT)* *Security Providers Act 1993 (Qld)* *Security and Investigation Industry Act 1995 (SA)* *Security and Investigations Agents Act 2002 (Tas)* *Private Security Act 2004 (Vic)* *Security and Related Activities (Control) Act 1996 (WA)* **Standards**: AS/NZS ISO 31000:2009 Risk management - Principles and guidelines AS/NZS 4421:2011 Guard and Patrol Security Service
Read in conjunction with	Base Services Contract Base Security Plans
See also DSPF Principle(s)	Defence Industry Security Program Identity Security Access Control Identification, Search and Seizure Regime Procurement
Implementation Notes, Resources and Tools	Australian Government physical security management protocol Australian Government physical security management protocol ASIO, Security Equipment Guides (SEGs) are available to ASAs from the GovDex Protective Security Community Defence Industry Security Program (Industry Security)

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

Defence Security Principles Framework (DSPF)

Contracted Security Guards

Control Owner

1. Director General Estate Service Delivery (DG ESD) is the owner of this enterprise-wide control.

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager.
Moderate	EL2 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations.
Significant	DG ESD
High	Defence Security Committee (DSC) – through First Assistant Secretary Service Delivery (FAS SD).
Extreme	DSC – through FAS SD.

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Control

Probity and Security Checking

2. **Licences**. Contracted Security Guards, including employees and sub-contractors of contracted guarding service providers, are to maintain current State/Territory licences to carry out their required functions.

3. **Personnel security clearance**. Contracted security guards are to hold a minimum security clearance of Baseline whilst engaged on the Defence Estate. Higher clearances may be required for facility-specific duties.

4. **Defence Industry Security Program (DISP) Membership**. Contracted security providers are to maintain DISP membership (refer DSPF Principle 16 - *Defence Industry Security Program*).

Contract Requirements

5. Contract Managers are to ensure contracted security guards are contractually required to:

a. be licensed in the relevant State/Territory;

b. display their security licence on their person whilst on duty;

c. maintain a minimum security clearance of Baseline; and

d. understand their responsibilities and obligations under, and not contravene, any Defence directives or Federal/State/Territory/local laws.

6. Contract Managers are to consult with the Defence Security & Vetting Service (DS&VS) regarding guarding contracts, prior to signature.

7. Incorporated security performance measures should focus on outcomes and support a risk management methodology (refer ISO 31000:2009 Risk Management – Principles and Guidelines.)

8. Contractors, Consultants and Outsourced Service Providers providing guarding services outside of Base Service guarding contracts are required to comply with the licencing and training requirements in this DSPF Control in addition to anything specified in their contracts.

Competencies

9. People engaged as contracted security guards are to possess a minimum Certificate II in Security Operations.

10. Contracted security guards are to maintain the required competencies throughout their employment whilst engaged on the Defence estate.

11. Contracted security guards carrying out specialist functions may be required to obtain and maintain a Certificate III in Security Operations in addition to additional competencies.

12. Contracted security guards are to complete a Defence-endorsed training package (delivered by the contracted security guard service provider, or Defence). This is to cover topics such as:

a. Defence security policy and relevant Federal, State and Territory laws;

b. Defence protocols (including rank structure, customer service, etc.);

c. the Defence security environment;

d. Defence policing; and

e. the SAFEBASE alert level security system.

Guarding Duties and Assignment Instructions

13. Contracted security guards are to be given comprehensive, base-specific assignment instructions that include:

a. the effective security of the base or facility;

b. dealing with emergency procedures;

c. lines of communication; and

d. accountabilities.

14. The Director Base Security Operations (DBSO) is to ensure contracted security guards are familiar with their assignment instructions, and all operational practices and procedures.

15. Assignment instructions are to address the responsibilities of contracted security guards as agents of the Commonwealth in relation to legal powers under the *Crimes Act 1914* and *Defence Act 1903*. These include:

a. the granting or refusing of entry;

b. the right of challenge;

c. common law arrest; and

d. search in relation to offences.

16. The instructions are to be endorsed by the control owner in consultation with local Base Support Managers (BSMs), and should be reviewed annually. They should also be reviewed when:

a. There is a change to the SAFEBASE alert level (refer DSPF Principle 83 - *SAFEBASE*); or

b. infrastructure changes occur.

17. These instructions are to be available for contracted security guards to consult in the course of their duties, but secured in line with DSPF Principle 10 – *Classification and Protection of Official Information*.

18. The DBSO and the contracted security provider are to be consulted prior to any changes to Base Security Instructions or the operation of physical security equipment being implemented. Any enhancements are to be delivered with adequate notice and training.

Other site specific duties

19. Other duties contracted security service providers and guards may be required to undertake at designated sites include, but are not limited to:

a. controlling access points;

b. issuing, receipting, encoding and recording Defence Common Access Cards (DCAC) and other Defence identity and access cards (refer to DSPF Principle 74 – *Access Control*);

c. conducting consensual identification and search, and restraint and detention in defined circumstances (refer to DSPF Principle 76 - *Identification, Search and Seizure Regime*);

d. conducting patrols of sites, perimeters and building exteriors (including providing, operating and maintaining electronic patrol recording systems);

e. operating and resetting (including arming and disarming) alarm panel systems;

f. monitoring and operating alarm control systems, including:

   i. following alarm response instructions;

   ii. conducting alarm verification and acknowledgement;

   iii. closing alarm incidents; and

   iv. reporting alarm incidents.

g. operating and monitoring surveillance and detection systems;

h. operating emergency response systems, including Base Wide Audible Alert Systems;

i. responding to security incidents;

j. managing security keys including:

   i. maintaining a registry for all allocated security keys;

   ii. ensuring the security of keys and key management systems;

iii. issuing and receipting security keys; and

iv. reporting lost or suspected compromised keys to Base Support personnel.

k. reporting and recording security and patrol incidents and occurrences, including security-related damage;

l. contributing to the investigation of security incidents; and

m. providing reports and audits in accordance with contractual regimes.

Patrols and alarm response

20. Contracted guarding services may include mobile and random patrols of bases outside of business hours, even if the site has a 24/7 security guard presence. Requirements for mobile patrols (including their frequency) are to be determined through a Security Risk Assessment (SRA).

21. The frequency of patrols undertaken for regular information container or physical asset inspections, and patrols of facilities out of hours are defined by guidelines:

a. provided by ASIO in the ASIO - Type 1 SAS – Implementation and Operation Guide (refer to Table 1 – Out of hours patrol and alarm response requirements);

b. in the Protective Security Policy Framework (PSPF) Physical Security Risk Management Guidelines: Security Zones and risk mitigation control measures: Section 5.8.1 Out of hours guarding; and

c. requirements defined in any SRAs.

Table 1 – Out of Hours Patrol and Alarm Response Requirements

Physical Security Zone	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
Out of hours guard patrols (random intervals)	Determined by SRA	Determined by SRA	Minimum every 4 hours	Minimum every 4 hours	Minimum every 2 hours
Out of hours alarm response	As contained in SRA.	As contained in SRA.	Determined by SRA (response should be within the delay period given by the physical security controls)	Determined by SRA (response should be within the delay period given by the physical security controls)	Determined by SRA (response should be within the delay period given by the physical security controls)

22. Out-of-hours contracted security guards, in response to alarms in all Physical Security Zones, are to respond within the delay period afforded by the physical security controls.

Roles and Responsibilities

Director General Estate Service Delivery (DG ESD)

23. DG ESD is responsible for:

a. the delivery of contracted guarding services to Defence bases in the Base Accountabilities Model; and

b. approving the requirement for specialist guarding functions at a base or facility.

Group Heads and Service Chiefs

24. In the unlikely event that guarding services are required to be engaged outside of the national contract, Group Heads and Service Chiefs are to ensure:

a. guarding requirements (including those in this DSPF Control) are incorporated into any guarding contracts;

b. contract performance is monitored and assessed;

c. the service provider is a member of the Defence Industry Security Program (DISP); and

d. E&IG is consulted in the development of security guarding contracts and arrangements.

Contract Managers

25. Contract Managers are responsible for ensuring:

a. guarding requirements are identified (including the requirement for surge as directed by Defence), and are appropriately included in the contract;

b. the guarding standards in this DSPF Control and E&IG SOPs are incorporated into security guarding contracts;

c. contracts for the provision of guarding services allow for changing requirements and changes to the SAFEBASE alert level;

d. contract performance is monitored and assessed;

e. the contracted security provider is a member of the DISP;

f. external service providers are contractually bound to comply with AS/NZS 4421:2011; and

g. DS&VS is consulted in the development of security guarding contracts.

Base Support Manager

26. The BSM, in consultation with the Senior ADF Officer (SADFO), and as a part of the base SRA, is responsible for consulting with the Contract Manager to determine guarding requirements at their base.

27. The BSM is also responsible for:

a. ensuring effective communication:

   i. the BSM;

   ii. SADFO; and

   iii. any other base security personnel that support incident response arrangements, and the management of other contracted guarding functions;

b. ensuring there effective management arrangements are in place to coordinate and task guards in response to a security threat, an incident, or a change to the SAFEBASE alert level;

c. maintaining oversight of guarding services and ensuring all guarding requirements and standards are met;

d. establishing base security instructions; and

e. involving contracted security providers in planning activities and site reviews.

Key Definitions

28. **Security Guard**: A person tasked to undertake guarding functions, including:

a. access control (e.g. reception, pass issue, patrols, traffic control, and search and inspection);

b. asset and alarm monitoring;

c. responding to security incidents;

d. operating alert and communications systems; and

e. security administration.

29. **Assignment Instructions**: An operational document detailing the specific duties to be performed under a guarding contract.

Further Definitions

30. Further definitions for common PSPF terms can be found in the Glossary.

31. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

This DSPF Control has no Annexes or Attachments.

Document Administration

Identification

DSPF Control	Contracted Security Guards
Control Owner	DG ESD
DSPF Number	Control 75.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise- wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Contracted Security Guards
Related DSPF Control(s)	Defence Industry Security Program Identity Security Access Control Identification, Search and Seizure Regime Procurement

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	DG ESD	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Identification, Search and Seizure Regime

General principle

1. Defence controls access to Defence facilities, assets and official information through an identification, search and seizure regime in full compliance with the relevant legislation.

Rationale

2. Security precautions at Defence bases aim to protect people, prevent theft and damage to Defence assets and infrastructure, and prevent unauthorised access to sensitive Defence information and systems. A key component of these precautions is the implementation of a statutory identification, search and seizure regime.

Expected outcomes

3. Defence operates a statutory regime of graduated identification, search, seizure and related powers, which are exercised by three identified classes of Defence Security Officials, to enhance the security of Defence bases, facilities, assets and personnel within Australia.

4. The level of identification and search capability required at each Defence site is determined on the basis of a security risk assessment, having regard to the nature of the primary assets to be protected and the assessed security risks.

Note: *A different search regime may operate on Defence bases where Defence Security Official's (DSO) are not utilised. Searches undertaken outside of the Defence Act 1903 Part VIA may be based on common law or other legislation and are strictly limited in scope. Further information on searches conducted under these circumstances is provided at DSPF Control 76.1, Annex A - Other Non-Statutory Search Regimes.*

Escalation Thresholds

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations
Significant	Director General (DG) ESD
High	Defence Security Committee (DSC) – through First Assistant Secretary, Service Delivery Division (FAS SD)
Extreme	DSC – through FAS SD

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Identification, Search and Seizure Regime
Control Owner	Director General Estate Service Delivery
DSPF Number	Principle 76
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry

Related information

Government Compliance	**PSPF Core Requirements**: Entity physical resourses. **Legislation**: *Defence Act 1903*, Part VIA, Security of Defence Premises.
Read in conjunction with	Access Control
See also DSPF Principle(s)	Physical Security Certification and Accreditation Security Incidents and Investigations
Implementation Notes, Resources and Tools	The scope of this principle and underlying security controls is confined to describing the identification search and seizure regime and does not describe the role of Armed Security Wardens or the operation of the Enhanced Self Defence Capability (ESDC) – these remain the responsibility of the Chief of Army (CA). Australian Government physical security management protocol

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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Identification, Search and Seizure

Control Owner

1. The Director General Estate Service Delivery (DG ESD) is the owner of this enterprise-wide control.

Escalation Thresholds

2. The DG ESD 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 Estate and Infrastructure Group, Service Delivery Division (SD), Estate Service Delivery (ESD), Directorate Base Security Operations
Significant	DG ESD
High	Defence Security Committee (DSC) – through First Assistant Secretary, Service Delivery Division (FAS SD)
Extreme	DSC – through FAS SD

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Implementation of Identification, Search and Seizure Regime

3. Implementation of the identification, search and seizure regime and the subsequent appointment of Defence Security Officials (DSO) across Defence premises will vary depending upon the nature of the site, the primary assets to be protected and the threat level. For example:

a. Consensual search and identification actions might be undertaken by contracted Defence security guards, on entry to and exit from Defence premises, or part thereof, at low to medium SAFEBASE alert levels.

b. Non-consensual identification, search and seizure actions might be undertaken by security authorised Defence Force members or, by Defence security screening employees if it is not reasonably practical for a security authorised Defence Force member to do so, during higher SAFEBASE alert levels, in response to a specific security incident or at any other time if warranted by specific circumstances.

Note: *Further information on the application of the identification search and seizure regime at different SAFEBASE levels is contained in DSPF Principle 83 - SAFEBASE.*

4. The Base Support Manager (BSM) and the Senior Australian Defence Force Officer (SADFO) are jointly responsible for providing a recommendation to the DG ESD on the implementation of the identification search and seizure regime at their base. This recommendation should be based on a security risk assessment of the site. The planned operation of the identification search and seizure regime should be addressed in the Base Security Plan.

5. For Offences and Penalties that relate to this DSPF part refer to Annex B to DSPF Control 76.1 - *Offences and Penalties*.

Defence Security Officials

6. The *Defence Act 1903 (Cth)* (*the Act*) establishes three categories of DSO that are authorised to exercise some or all of the powers conferred by Part VIA of the Act. A DSO may be:

a. a contracted Defence security guard (Contractor);

b. a Defence security screening employee (Australian Public Service (APS) Employee); or

c. a security authorised member of the Defence Force.

Note: *In accordance with the Defence Act 1903, a Security Officer cannot exercise any of the identification, search and seizure powers unless they have been authorised to do so by the Minister as a DSO.*

7. Table 1 shows the relationship between the various terms used to describe a DSO.

Table 1 – Categories of Defence Security Officials

Contracted Defence Security Guard	**Special Defence Security Official (SDSO)**	
	Defence Security Screening Employee	**Security Authorised Member of the Defence Force:** • Identification and Search Warden • Military Working Dog Handler • Armed Security Warden

8. The powers that can be exercised by each category of DSO are summarised at Annex E to DSPF Control 76.1 - *Summary of Defence Security Officials' Powers*.

Contracted Defence Security Guard

9. A contracted Defence security guard is a contractor, subcontractor or their employee, who provides security services at Defence premises under a contract with the Commonwealth, and has been authorised by the Minister, by written instrument, to be a contracted Defence security guard. The Minister will only authorise as contracted Defence security guards, individuals who have met a standard of security training and qualification requirements as determined by the Minister, or his delegate, in a legislative instrument. This training should include scenario based training to provide guidance on the exercise of powers by contracted Defence security guards. For further information on training and qualification requirements refer to DSPF Principle 75 – *Contracted Security Guards*, and Annex D to DSPF Control 76.1 *Defence Security Officials – Training and Qualification Requirements*.

10. Under the *Defence Act 1903* (refer to Part VIA, Division 3) and this DSPF part, contracted Defence security guards are only authorised to:

a. request or require evidence of a person's identification and authority to pass an access control point or be on Defence premises;

b. conduct consensual limited searches of a person (including items in the person's possession);

c. conduct consensual searches of vehicles; and

d. in specified circumstances, restrain and detain a person for the purposes of placing them in the custody of a Federal, State or Territory Police officer.

Note: *All references to contracted Defence security guards in this DSPF part refer to contracted security guards who have been authorised by the Minister as contracted Defence security guards under the Act. Security guards, who work at Defence sites that have not been authorised by the Minister, cannot exercise the powers conferred by Part VIA of the Act.*

Defence Security Screening Employees

11. A Defence security screening employee is an APS employee of the Department of Defence who has been authorised by the Minister, by written instrument, to be a Defence security screening employee. The Minister will only authorise as Defence security screening employees, APS employees who have met a standard of security training and qualification requirements as determined by the Minister, or his delegate, in a legislative instrument. This training should include scenario based training to provide guidance on the exercise of powers by Defence security screening employees[2].

12. Defence security screening employees must have volunteered to undertake the additional responsibilities and risks associated with this role, or occupy a position where these additional responsibilities are included in the duty statement.

13. Under the *Defence Act 1903* (refer to Part VIA, Division 3) and this DSPF part, Defence security screening employees are authorised to:

a. request evidence of a person's identification and authority to pass an access control point or be on Defence premises;

b. conduct consensual limited searches of a person (including items in the person's possession);

c. conduct consensual searches of vehicles; and

d. in specified circumstances, restrain and detain a person for the purposes of placing them in the custody of a Federal, State or Territory Police officer.

14. In circumstances where it is not reasonably practicable for a security authorised member of the Defence Force to do so, Defence security screening employees are further authorised under the *Defence Act 1903* (refer to Part VIA, Divisions 4 and 5) to:

a. require evidence of a person's identification and authority to be on Defence premises;

[2] For further information on Training and Qualification requirements refer to Annex D to DSPF Control 76.1 - *Defence Security Officials – Training and Qualification Requirements*.

b. conduct non-consensual searches of a person (including items in the person's possession) and non-consensual vehicle searches; and

c. in specified circumstances:

i. request a person to leave the premises and, if they refuse, remove the person from the premises with reasonable force if required;

ii. restrain and detain a person (applying reasonable force) for the purposes of placing them in the custody of a Federal, State or Territory Police officer; and

iii. seize items that are a threat to safety or relate to a criminal offence for the purpose of transferring custody to the Australian Federal Police (AFP) or Police Force of a State or Territory.

Security Authorised Member of the Defence Force

15. A security authorised member of the Defence Force is an Australian Defence Force (ADF) member who has been authorised by the Minister, by written instrument, to be a security authorised member of the Defence Force. The Minister will only authorise as security authorised members of the Defence Force, ADF members who have met a standard of security training and qualification requirements as determined by the Minister, or his delegate, in a legislative instrument. This training should include scenario based training to provide guidance on the exercise of powers by security authorised members of the Defence Force.

16. Different training and qualification requirements apply to specialised sub-categories of security authorised Defence Force members, for example Identification and Search Wardens (ISW), Military Working Dog Handlers and Armed Security Wardens[3].

Note: *The exercise of powers by Armed Security Wardens[4] is limited to circumstances where an attack on Defence premises is imminent or occurring. For further guidance on Armed Security Wardens refer to DSPF Principle 83 - SAFEBASE.*

[3] For Further information on Training and qualification requirements refer to Annex D to DSPF Control 76.1 - *Defence Security Officials – Training and Qualification Requirements*.

[4] Armed Security Wardens are part of the Enhanced Self-Defence Capability as managed by the Chief of Army.

17. Under the *Defence Act 1903* (refer to Part VIA Divisions 3, 4 and 5) and this DSPF part, security authorised members of the Defence Force, who are trained and qualified as ISW, are authorised to:

a. request or require evidence of a person's identification and authority to pass an access control point or be on Defence premises;

b. conduct consensual limited searches of a person (including items in the person's possession) and consensual vehicle searches;

c. conduct non-consensual searches of a person (including items in the person's possession) and non-consensual vehicle searches; and

d. in specified circumstances:

   i. request a person to leave the premises and, if they refuse, remove the person from the premises using reasonable force;

   ii. restrain and detain (applying reasonable force when required) a person for the purposes of placing them in the custody of a Federal, State or Territory Police officer to exercise their powers of arrest;

   iii. seize items that are a threat to safety or relate to a criminal offence for the purpose of transferring custody to the AFP or Police Force of a State or Territory; and

   iv. take action to make seized items safe or prevent their use.

Authorisation of Defence Security Officials

18. In accordance with the *Defence Act 1903*, before exercising any powers provided under Part VIA, a DSO **must**:

a. complete the specified training and hold the requisite qualifications associated with his/her category (or sub-category) of security official as determined by the Minister, or the Minister's delegate, in a legislative instrument[5];

b. be authorised to be a contracted Defence security guard, a Defence security screening employee or a security authorised Defence Force member by the Minister; and

[5] For Further information on Training and qualifications refer to Annex D to DSPF Control 76.1 - *Defence Security Officials – Training and Qualification Requirements*.

c. be issued with an identity card by the Secretary or the Secretary's delegate.

19. A DSO may have their authority to exercise powers under the *Defence Act 1903* temporarily revoked, for example, if the DSO is being investigated in relation to the possible commission of an offence under the *Defence Act 1903*. Refer to Annex B to DSPF Control 76.1 - *Offences and Penalties* for further information on offences. In these circumstances, the DSO is required to return their identity card to an authorised delegate until the matter is resolved within 7 days of being notified. Refer to Annex F to DSPF Control 76.1 - *Defence Security Official Identity Cards (DSOIC)* for further information.

Identification of Defence Security Officials

20. In accordance with the *Defence Act 1903*, Part VIA section 71E, Defence Security Officials (DSO) **must** carry an identity card at all times when performing functions or exercising their powers under Part VIA. In addition, under Section 72B of Part VIA of the Act, a DSO **must** produce this card for inspection by a person before:

a. requesting or requiring the person to provide evidence of their identification or authority to pass an access control point or be on Defence premises;

b. requesting a consensual limited search of a person (including items in the person's possession) or a consensual search of a vehicle apparently under the person's control;

c. requiring a non-consensual search of the person (including items in the person's possession) or a vehicle apparently under the person's control; or

d. restraining, detaining or removing the person from Defence premises.

Note: *If a SDSO reasonably believes that a person constitutes a threat to safety such that complying with this requirement, prior to conducting a non-consensual search, places the safety of the official and others at risk, they may temporarily delay presenting their identity card. For example, this might occur if the official reasonably believes the person is carrying a concealed weapon. In these circumstances, after the immediate threat to safety has been resolved, the official is required to produce their identity card for inspection by the person and inform the person of the effect of hindering or obstructing the search*[6]*.*

[6] Further information on the production and management of identity cards for DSOs refer to Annex F to DSPF Control 76.1 - *Defence Security Official Identity Cards (DSOIC)*.

Identification Powers

21. A DSO is authorised to request evidence of a person's identification or authority to be on Defence premises, when:

a. a person is entering or exiting Defence premises, or part of Defence premises, through an access control point; or

b. a person is on Defence premises (i.e. at areas other than an access control point) and the DSO reasonably believes that the person is not authorised to be there.

22. Further, a SDSO may require a person to present evidence of their identification or authority to be on Defence premises, when:

a. a person is entering or exiting Defence premises, or part of Defence premises, through an access control point; or

b. a person is on Defence premises (i.e. at areas other than an access control point) and the SDSO reasonably believes the person:

i. is not authorised to be on the premises;

ii. constitutes a threat to the safety of people on the premises; or

iii. has or may commit a criminal offence on, or in relation to the premises.

23. When requesting or requiring a person to produce identification, all DSOs are required to produce their identity card for inspection and inform the person of the consequences of refusing to comply with the request or requirement.

Consensual Identification Powers

Consensual Identification of a Person at Access Control Points

24. Under the *Defence Act 1903* Part VIA section 71H, a DSO may request a person who is about to pass an access control point to provide evidence of their identity and authority to pass the access control point.

25. Further, a DSO may refuse to allow a person to pass an access control point and, if on Defence premises, restrain and detain the person, if:

a. the person refuses the identification request or fails to provide evidence that satisfies the DSO; or

b. as a result of complying with the request, the DSO reasonably believes that the person:

i. is not authorised to pass the access control point;

ii. constitutes a threat to the safety of people on the premises; or

iii. has or may commit a criminal offence on, or in relation to, the premises.

26. If the circumstances described above occur when a person is seeking to enter a Defence premises, or a part of the premises, a DSO is to refuse the person entry in accordance with Defence's policy on access control. For further information refer to DSPF Principle 74 - *Access Control*.

Consensual Identification of a person on Defence Premises

27. Under the *Defence Act 1903* Part VIA section 71K a DSO may request a person, who is on Defence premises (ie at areas other than access control points), and who the DSO reasonably believes is not authorised to be there, to provide evidence of their identity and authority to be on the premises.

Example: *It would be reasonable for a DSO to conclude that a person on Defence premises, who is not visibly wearing a Defence access or identity card, is not authorised to be there. As a result, the official would be entitled to stop the person and request that they provide evidence of their identification and authority to be on the premises.*

28. Further, a DSO may restrain and detain a person, if:

a. the person refuses the identification request or fails to provide evidence that satisfies the DSO; or

b. as a result of complying with the request, the DSO reasonably believes that the person:

i. is not authorised to be on the premises;

ii. threat to the safety of people on the premises; or

iii. has or may commit a criminal offence on, or in relation to the premises.

Refusal to Comply with a Consensual Identification Request

29. A person's refusal or failure to comply with a request from a DSO to provide evidence of their identity and authority to pass an access control point or be on Defence premises does not constitute an offence. However, in these circumstances, the DSO is to deny the person entry to Defence premises and, if the person is already on the premises, may restrain and detain the person for the purposes of placing them into the custody of a Federal, State or Territory Police officer for trespass or other criminal offences. The DSO is to contact police as soon as

practicable after a person has been restrained and detained. The authority to restrain and detain in these circumstances is outlined in this part. For further information on restrain and detain powers refer to "*Restrain and Detain Powers*" in this part.

30. Under the *Defence Act 1903* Part VIA section 71T, if a SDSO reasonably believes that a person, who has been restrained and detained in the circumstances outlined above, constitutes a threat to the safety of persons on Defence premises, they may conduct a non-consensual identification and search of the person while awaiting the arrival of police.

Non-consensual Identification Powers

31. Under the *Defence Act 1903* Part VIA section 71Y, a SDSO may stop and detain a person or vehicle for the purposes of requiring a person to present evidence of their identification or authority to be on Defence premises.

Non-consensual Identification of a Person at Access Control Points

32. Under the *Defence Act 1903* Part VIA section 71R, a SDSO may require a person who is about to pass an access control point to provide evidence of their identity and authority to pass the access control point.

33. Further, the SDSO may refuse to allow a person to pass the access control point, if:

a. the person refuses the identification requirement or fails to provide evidence that satisfies the DSO; or

b. as a result of complying with the requirement, the DSO reasonably believes that the person:

   i. is not authorised to pass the access control point;

   ii. constitutes a threat to the safety of people on the premises; or

   iii. has or may commit a criminal offence on, or in relation to the premises.

34. If the SDSO refuses to allow a person to pass an access control point and the person is on Defence premises, the SDSO may:

a. restrain and detain the person, or

b. request the person to leave the premises and, if he or she refuses, remove the person from the premises.

35. If the circumstances described above occur when a person is seeking entry to Defence premises, or part of the premises, an SDSO is to refuse the person entry in accordance with Defence's policy on access control and identity management[7].

Non-consensual Identification of a Person on Defence Premises

36. Under the *Defence Act 1903* Part VIA section 71T, a SDSO may require a person, who is on Defence premises (ie at areas other than access control points), to provide evidence of their identity and authority to be on the premises, if the official reasonably believes that the person:

a. is not authorised to be on the premises;

b. constitutes a threat to the safety of people on the premises; or

c. has or may commit a criminal offence on, or in relation to the premises.

Example: *It would be reasonable for a SDSO to conclude that a person on Defence premises who is not visibly wearing a Defence access or identity card is not authorised to be there. As a result, the official would be entitled to stop the person and require that they provide evidence of their identification and authority to be on the premises.*

37. Further, a SDSO may restrain and detain a person, or request a person to leave the premises and, if he or she refuses, remove the person from the premises (reasonable force may be applied), if:

a. the person refuses the identification requirement or fails to provide evidence that satisfies the DSO; or

b. as a result of complying with the request, the SDSO reasonably believes the person:

   i. is not authorised to be on the premises;

   ii. constitutes a threat to the safety of people on the premises; or

   iii. has or may commit a criminal offence on, or in relation to the premises.

[7] For further information on identity management refer to the DSPF Principle 74 - *Access Control*.

Search Powers

38. A DSO is authorised to conduct a consensual limited search of a person (including items in the person's possession) and a consensual search of a vehicle (including things in the vehicle), when a person or vehicle is entering or exiting Defence premises, or part of Defence premises, through an access control point.

39. Further, a SDSO is authorised to conduct a non-consensual search of a person (including items in the person's possession) or a vehicle (including things in the vehicle), when:

a. a person or vehicle is about to pass an access control point that is located on Defence premises; or

b. a person or vehicle is on Defence premises (i.e. at areas other than an access control point) and the SDSO reasonably believes the person or vehicle:

   i. is not authorised to be on the premises;

   ii. constitutes a threat to the safety of people on the premises;

   iii. in the case of a person, has or may commit a criminal offence on, or in relation to the premises; or

   iv. in the case of a vehicle, relates to a criminal offence that has or may be committed on, or in relation to the premises.

40. At declared explosive ordnance depots, contracted Defence security guards are further authorised to conduct a consensual limited search of a person and a consensual search of a vehicle, if the person or vehicle is located anywhere on the depot, not just at the access points.[8] DSO are not authorised to undertake consensual or non-consensual searches of people, items or vehicles on Defence accommodation.

Note: *This restriction on the exercise of consensual and non-consensual search powers applies even if the accommodation is located within Defence premises.*

41. Prior to exercising their powers of search, a DSO is required to produce his or her identity card for inspection and inform the person of the consequences of

[8] For further information on declared explosive ordnance depot special search provisions refer to Annex G to DSPF Control 76.1 - *Special Search Provisions for Declared Explosive Ordnance Depots*.

refusing to comply with a request for a consensual search or a requirement to submit to a non-consensual search.

Note: *If an SDSO reasonably believes that a person constitutes a threat to safety such that complying with this requirement, prior to conducting a non-consensual search, places the safety of the official and others at risk, they may temporarily delay presenting their identity card. For example, this might occur if the official reasonably believes the person is carrying a concealed weapon. In these circumstances, after the immediate threat to safety has been resolved, the official is required to produce his or her identity card for inspection by the person and inform the person of the effect of hindering or obstructing the search.*

42. Contracted Defence security guards must conduct consensual limited searches of people and consensual searches of vehicles in accordance with the procedures detailed in their assignment instructions.[9]

43. SDSO must conduct all consensual and non-consensual searches of people and vehicles in accordance with the Standard Operating Procedures (SOPs) developed and held by Estate & Infrastructure Group (E&IG) to support the identification, search and seizure regime.

Consensual Search Powers

Consensual Searches at Access Points

44. Under the *Defence Act 1903* Part VIA section 71H, a DSO may request a person, who is about to pass an access control point, to undergo a consensual limited search of their person, including items in their possession.

45. Under the *Defence Act 1903* Part VIA section 71J, a DSO may request a person, who is apparently in control of a vehicle that is about to pass an access control to point, to permit a consensual search of the vehicle, including things in the vehicle.

46. Further, a DSO may refuse to allow a person or vehicle to pass an access control point and, if on Defence premises, restrain and detain the person and any other people in the vehicle, if:

a. the person refuses the consensual search request; or

b. as a result of complying with the request, the DSO reasonably believes that the person or the vehicle (including a thing in the vehicle):

   i. is not authorised to pass the access control point;

[9] For further information on assignment instructions for guards refer to DSPF Principle 75 - *Contracted Security Guards*.

ii. constitutes a threat to the safety of people on the premises;

iii. in the case of a person, has or may commit a criminal offence on, or in relation to the premises; or

iv. in the case of a vehicle, relates to a criminal offence that has or may be committed on, or in relation to the premises.

47. If the circumstances described within paragraph 46 of this part - "*Consensual Search Powers*" occurs when a person or vehicle is seeking entry to a Defence premise, or a part of the premises, a DSO is to refuse the person entry.

Note: *At declared explosive ordnance depots, contracted Defence security guards are further authorised to conduct a consensual limited search of a person and a consensual search of a vehicle, if the person or vehicle is located anywhere on the depot, not just at the access points[10].*

Refusal to Comply with a Consensual Search Request

48. A person's refusal to comply with a consensual search request from a DSO at an access control point does not constitute an offence. However, in these circumstances, the DSO is to deny the person entry to Defence premises and, if the person is already on the premises, may restrain and detain the person for the purposes of placing them in Federal, State or Territory police officer custody. The DSO must contact police as soon as practicable after the person has been restrained and detained. The authority to restrain and detain in these circumstances is outlined in paragraphs 44 to 46 of this part - "*Consensual Search Powers*".[11]

49. Under the *Defence Act 1903* Part VIA section 71T, if an SDSO reasonably believes that a person, who has been restrained and detained in the circumstances outlined above, constitutes a threat to the safety of persons on Defence premises, they may conduct a non-consensual search of the person while awaiting the arrival of police.

[10] For further information on Special Search Provisions for Declared Explosive Ordnance Depots refer to Annex G to DSPF Control 76.1 - *Special Search Provisions for Declared Explosive Ordnance Depots*.

[11] For further information on restrain and detain powers refer to "*Restrain and Detain Powers*" within this DSPF part at paragraphs 110 to 120.

Non-consensual Search Powers

50. Under the *Defence Act 1903* Part VIA section 71Y, a SDSO may stop and detain a person or vehicle for the purposes of conducting a non-consensual search of a person or vehicle.

Non-consensual Search of a Person at Access Control Points

51. Under the *Defence Act 1903* Part VIA section 71R, a SDSO may require a person, who is about to pass an access control point that is on Defence premises, to submit to a non-consensual search of their person, including items in their possession. This may be required when a person is exiting Defence premises through an access control point, or when entering or exiting an area within the premises through an internal access control point.

Note: *If the access control point is located at the external perimeter of the Defence base or site, a SDSO cannot require a person to undergo a non-consensual search on entry. In these circumstances, a DSO can request the person to undergo a consensual limited search.*[12]

52. Further, the SDSO may refuse to allow a person to pass the access control point, if:

a. the person hinders or obstructs the non-consensual search; or

b. as a result of the search, the SDSO reasonably believes that the person:

   i. is not authorised to pass the access control point;

   ii. constitutes a threat to the safety of people on the premises; or

   iii. has or may commit a criminal offence on, or in relation to the premises.

53. If the SDSO refuses to allow a person to pass an access control point, the SDSO may:

a. restrain and detain the person; or

b. request the person to leave the premises and, if he or she refuses, remove the person from the premises (reasonable force may be used).

---

[12] For further information on consensual limited search refer to "*Consensual Search Powers*" within this DSPF part at paragraphs 44 to 46.

54. If the circumstances described within paragraph 53 of this part - "*Access Control Points*", occurs when a person is seeking entry to an area within the Defence premises through an access control point (i.e. other than an access control point located at the external perimeter of a base), an SDSO should refuse the person entry.

Non-consensual Search of a Vehicle at Access Control Points

55. Under the *Defence Act 1903* Part VIA section 71S, a SDSO may require a person, who is apparently in control of a vehicle that is about to pass an access control point that is located on Defence premises, to permit a non- consensual search of the vehicle, including things in the vehicle. This may be required when the vehicle is exiting Defence premises through an access control point, or when the vehicle is entering or exiting an area within the premises through an access control point.

Note: *If the access control point is located at the external perimeter of the Defence base or site, a SDSO cannot require a person to submit to a non-consensual vehicle search on entry. In these circumstances, a DSO can request the person to permit a consensual vehicle search[13].*

56. The SDSO may refuse to allow a vehicle to pass the access control point, if:

a. a person hinders or obstructs the non-consensual search; or

b. as a result of the search, the SDSO reasonably believes that the vehicle (including a thing in the vehicle):

   i. is not authorised to pass the access control point;

   ii. constitutes a threat to the safety of people on the premises; or

   iii. relates to a criminal offence that has or may be committed on, or in relation to the premises.

57. If the SDSO refuses to allow a vehicle to pass an access control point, the SDSO may restrain and detain any people in the vehicle.

Non-consensual Search of a Person on Defence Premises

58. Under the *Defence Act 1903* Part VIA section 71T, a SDSO may require a person, who is on Defence premises (i.e. at areas other than access control points),

[13] For further information on non-consensual and consensual search of vehicles refer to "*Consensual Search Powers*" within this DSPF part at paragraphs 44 to 46.

to submit to a non-consensual search of their person, including items in their possession, if the official reasonably believes that the person:

a. is not authorised to be on the premises;

b. constitutes a threat to the safety of people on the premises; or

c. has or may commit a criminal offence on, or in relation to the premises.

59. Further, a SDSO may restrain and detain a person, or request a person to leave the premises and, if he or she refuses, remove the person from the premises, if:

a. the person hinders or obstructs the non-consensual search; or

b. as a result of the search, the SDSO reasonably believes that the person:

i. is not authorised to be on the premises;

ii. constitutes a threat to the safety of people on the premises; or

iii. has or may commit a criminal offence on, or in relation to the premises.

Non-consensual Search of a Vehicle on Defence Premises

60. Under the *Defence Act 1903* Part VIA section 71U, a SDSO may require a person, who is apparently in control of a vehicle that is located on the premises, to permit a non-consensual search of the vehicle, including things in the vehicle, if the official reasonably believes that the vehicle:

a. is not authorised to be on the premises;

b. constitutes a threat to the safety of people on the premises; or

c. relates to a criminal offence that has or may be committed on, or in relation to the premises.

61. Further, a SDSO may restrain and detain any person in the vehicle, if:

a. a person hinders or obstructs the non-consensual search; or

b. as a result of the search, the SDSO reasonably believes that the vehicle:

i. is not authorised to be on the premises;

ii. constitutes a threat to the safety of people on the premises; or

iii. relates to a criminal offence that has or may be committed on, or in relation to the premises.

Exemptions to Search Regime

62. It is in Defence's interests to facilitate the lawful activities of other officials when undertaking their statutory functions or responding to incidents on Defence premises. This might include:

a. civilian law enforcement personnel (including Customs and Border Protection Service Officers);

b. emergency services personnel; and

c. other Commonwealth government officials (e.g. Comcare inspectors).

63. Such officials are provided with a limited exemption from the search powers when performing their statutory duties. That is, prior to requesting the official undergo a consensual limited search of their person or vehicle, the DSO must reasonably believe that the official:

a. constitutes a threat to the safety of people on the premises; or

b. has or may commit a criminal offence on, or in relation to, the premises.

64. If, in the circumstances described within this DSPF part "Exemption To Search Regime" in paragraph 63 occurs and the official refuses to provide their consent, they must be treated the same as any other person who has not provided their consent.

65. A full exemption to the identification search and seizure regime must be provided to a person who has diplomatic status and who is accompanied by a Defence Force member or civilian employee of the Department.

66. The Base Commander, BSM or SADFO may determine whether other exemptions are warranted in specific situations.

Compensation

67. If an item is damaged as a result of a search and no criminal proceedings are instituted in relation to the item, or it is found not to have been involved in the commission of a criminal offence, compensation may be payable to the owner of the item.

68. Refer to Defence Legal for further information on compensation matters.

Seizure

69. Under the *Defence Act 1903* Part VIA section 72, a SDSO may seize an item that is on Defence premises, including a vehicle or an unattended item, or an item

that is found as a result of a consensual or non-consensual search, if the official reasonably believes that it may:

a. constitute a threat to the safety of people on the premises; or

b. relate to a criminal offence that has or may be committed on, or in relation to the premises.

70. Where the seizure relates to a possible security threat, a security authorised member of the Defence Force may take any action that is reasonable and necessary to make the seized item safe or prevent its use, for example, unloading a firearm. In respect of a suspicious item that is left unattended on the premises, this action could include a non-consensual search of the item to establish whether it constitutes a threat to the safety of people on the premises[14].

71. If a SDSO reasonably believes a seized item has been used or involved in the commission of a criminal offence, the official is required to hand the item over to the police at the earliest practicable time. This requirement, however, does not apply if action is necessary to make the item safe or prevent its use, and this action prevents the item from being provided to the police.

72. In the circumstances outlined above, the seized item cannot be transferred to the custody of a Protective Security Officer of the AFP. Any item believed to be involved in a criminal offence must be carefully handled in accordance with correct evidence management procedures to ensure potential evidential material is not inadvertently contaminated[15].

73. A SDSO should provide a person with a receipt for a seized item, if it is practicable to do so.

74. In the event that it is established that the seized item has not been used or otherwise involved in the commission of an offence, and as such there is no requirement to provide the item to the police, the SDSO should return the item to the person within seven days if it is practicable to do so or, if not, provide it to police.

Note: *A seized item that cannot be returned to the person within seven days cannot be handed over to a Protective Service Officer of the AFP.*

[14] Refer to extant emergency management procedures for further guidance in dealing with potentially threatening items.

[15] For handling evidential information or items refer to the Standard Operating Procedures (SOPs)

Additional Considerations

Use of Reasonable and Necessary Force

75. Under the *Defence Act 1903* section 72G, when exercising their powers under Part VIA, a DSO:

a. should only use such force against a person or thing as is reasonable and necessary; and

b. should not subject a person to greater indignity than is reasonable and necessary.

76. Reasonable force is regarded to be the minimum force reasonably necessary in the circumstances of a particular situation. That is, the use of force must be limited, in its intensity and duration, to that which is required to resolve the situation.

77. In potentially difficult situations, the DSO must attempt to reduce tension and resolve incidents without force or with a minimum use of force. The level of force must be graduated and appropriate to the level of threat faced.

78. If a DSO has used force against a person when exercising their powers under Part VIA of the *Defence Act 1903*, the official should ensure that the person receives medical attention if required.

79. In all cases where a DSO uses force against a person, he or she is to, as soon as practicable; submit a report setting out the full details of the force used and the circumstances in which the force was applied[16].

80. DSO may touch, as appropriate, a vehicle or item, or anything in a vehicle or item, in order to undertake a search.

Limit on Use of Force or Force Involving Death or Injury

81. The Australian Federal Police (AFP), or State/Territory police as applicable, has primacy during any attack on a Defence base that is imminent or in progress.

82. Under the *Defence Act 1903* Part VIA section 72G, a contracted Defence security guard or a Defence security screening employee should not use force against a person, or do anything that is likely to cause death or grievous bodily harm.

---

[16] Further information on reporting requirements refer to "*Reporting Requirements*" within this DSPF part at paragraphs 129 to 136.

Note: *Per section 72H, the use of force involving death or grievous bodily harm is strictly limited to Armed Security Wardens in circumstances where an attack on Defence premises, or people on Defence premises is imminent or occurring[17].*

Note: *In accordance with the Defence Act 1903 Part VIA section 72S, the Defence Act 1903 does not, by implication, limit the exercise of powers or rights of any person under the Defence Act 1903 or any other law. This includes the right to use force in defence of themselves or others.*

83. A DSO should not use force that is unwarranted or disproportionate to the situation. This includes situations where force has been used and:

a. no force was required;

b. more force was applied than was necessary;

c. the use of force continued after the necessity for it had ceased; or

d. force was knowingly and wrongfully used.

84. DSO may be criminally prosecuted for unreasonable use of force.

Exercise of Powers in relation to Protests etc.

85. Under the *Defence Act 1903* Part VIA section 72L, a DSO should not use their powers to stop or restrict any protest, dissent, assembly or industrial action, unless there is a reasonable likelihood of:

a. death or serious injury; or

b. the commission of a criminal offence.

Person to be Informed of Offence

86. Under the *Defence Act 1903* Part VIA section 72C if a DSO exercises their powers on the basis of a reasonable belief that the person has or may commit a criminal offence, the DSO is required to inform the person of the substance of the offence.

Note: *The language used may be general, rather than of a precise or technical nature.*

[17] For Further information on Armed Security Wardens refer to DSPF Principle 83 – *SAFEBASE*.

87. This requirement does not apply, however, if the person should, in the circumstances, know the substance of the offence or, through their actions, makes it impracticable for the official to inform the person of the offence.

Number of Defence Security Officials

88. Two DSO should be present during all searches to avoid any evidential dispute. In exceptional circumstances, such as a perceived threat to security or safety, a DSO may undertake a search without another DSO present.

Privacy

89. Where practicable, a person should be provided with the option of undergoing a consensual limited search or a non-consensual search of their person, including items in their possession, in a private area. Privacy could be provided by a screen or temporary structure.

90. In order to protect the privacy of the person, DSO are not to record or discuss anything of a private or personal nature observed or discovered during a search unless it is directly relevant to the identified reporting requirements or a perceived security or safety risk.

Vehicles

91. If possible, vehicles should be directed to vehicle search bays (if available) for the conduct of a search to ensure that routine vehicular traffic is not unnecessarily impeded.

Gender/Culture

92. Under the *Defence Act 1903* Part VIA Section 72D requires that a consensual limited search or non-consensual search of a person should, if practicable, be conducted by a DSO of the same gender as the person being searched. If a person is uncomfortable undergoing a search of their person, including items in their possession, by an official of the opposite gender they may choose to have another person (e.g. a colleague) present during the process. That person must be able to attend the search site in a timely manner.

93. All searches should be conducted in a culturally sensitive manner.

Security Construction and Equipment Committee (SCEC)

94. The contents of briefcases used for carrying classified material, are not exempt from being searched. If it is considered necessary to search a SCEC endorsed briefcase:

a. the briefcase can be opened and the contents given a cursory inspection to verify the existence of documented authorisation to carry the material (e.g. an

XC019 or XC051 form) and to ensure that the material has been properly protected and does not appear to have been subject to tampering;

b. the person carrying the briefcase can be asked to move papers and files around, but files must not be opened; and

c. classified material in a SCEC endorsed briefcase can only be seized by a SDSO.

Use of Equipment to Conduct Searches or Examine Items

95. Under the *Defence Act 1903* Part VIA section 72E, a DSO may use electronic and other devices, and obtain expert assistance, for the purposes of conducting a search of a person, item or vehicle or determining whether an item may be seized.

Example: *This may include, but is not limited to, the use of metal detectors, x-ray equipment, arthroscopic camera devices (to examine spaces that are confined or difficult to access such as areas of a vehicle engine bay), explosive residue equipment, chemical sniffers or other search devices.*

96. Further, the DSO may use equipment to gain access to data stored on items, for example data on laptops, mobile phones and thumb drives.

97. A search of an item should cease as soon as it has been established that there is a valid basis upon which to seize the item (e.g the discovery of a classified document on a laptop) and it has been determined that there is no immediate safety risk posed by the item/vehicle/person.

98. A DSO may move an item that is on Defence premises to another part of the premises for examination or processing, if the official suspects on reasonable grounds that the item:

a. constitutes a threat to the safety of people on the premises; or

b. relates to a criminal offence that has or may be committed on, or in relation to the premises.

99. Prior to utilising equipment to assist a search, a DSO must have completed training and maintain proficiency on that equipment.

Assistance to Defence Security Officials

100. Under the *Defence Act 1903* Part VIA section 72N, when exercising their powers, a DSO may be assisted by other people if it is reasonable and necessary to do so, to:

a. conduct a consensual search of a vehicle at an access control point;

b. conduct a consensual search of a vehicle on a declared explosive ordnance depot;

c. conduct a non-consensual search of a vehicle about to pass an access control point that is located on Defence premises;

d. conduct a non-consensual search of a vehicle located on Defence premises (ie at areas other than access control points);

e. use equipment to undertake a search of a person, item or vehicle; or

f. move things on Defence premises.

Example: *Assistance may be required to operate a forklift to unload a vessel, vehicle or aircraft so that a thorough search may be properly conducted by a DSO. Expert assistance may also be sought to use technical equipment to process an item.*

Note: *It would not be reasonable for a DSO to seek assistance to exercise powers that they have the capability, training, authorisation and physical capacity to exercise in their own capacity as a DSO.*

101. A person assisting a DSO may exercise the official's powers, but only in accordance with the directions of the DSO. Any person assisting a DSO who acts outside of the direction of a DSO may be individually liable for their actions.

102. Powers that are exercised by a person assisting a DSO are taken to have been exercised by the official. The DSO is liable for any misuse of power by a person assisting them to the extent that the person is following the direction of a DSO. That is, a DSO is not liable for any actions undertaken by a person assisting them if the person acted outside of the direction of the DSO.

Use of Military Working Dogs

103. Under the *Defence Act 1903* Part VIA section 72M, a security authorised member of the Defence Force may, if the member considers it is reasonably necessary, use a military working dog to:

a. assist a DSO to conduct a search or a limited search;

b. assist a DSO to restrain and detain a person, or remove a person from Defence premises;

c. assist an ADF member to arrest a person for trespass under section 72P of *the Act*; or

d. assist a DSO to perform a function or power under Part VIA of *the Act*.

104. Use of military working dogs is strictly limited to security authorised Defence Force members, who have completed the relevant training and qualification requirements as determined by the Minister for military working dog handlers. For further information on the training and qualification requirements refer Annex D to DSPF Control 76.1 - *Defence Security Officials – Training and Qualification Requirements*.

105. At all times, a military working dog handler should only use such force as is reasonable and necessary and direct their military working dogs in such a manner as to prevent unreasonable injury to people or damage to property

Move Items

106. A DSO may move an item (including a vehicle) that has been left unattended on Defence premises as a result of, or in connection with the exercise of a power under the *Defence Act 1903* Part VIA, if the DSO reasonably believes this action is necessary or desirable. For example, when a vehicle has been left unattended, after the driver has been restrained and detained, and the vehicle is impeding the normal operations of the premises or poses a traffic hazard.

107. If there is any suspicion that a vehicle or item poses a significant threat to safety, for example a suspicion that it may contain an improvised explosive device, a DSO must not attempt to move it and must contact the police immediately.

Storage

108. Where practicable, safe and secure storage facilities should be made available outside of Defence premises to allow people to securely store items that they do not want searched prior to entry. A DSO must ensure that people entering Defence premises are aware of the availability of storage facilities.

Signage

109. Notices should be prominently displayed at the entrance to all Defence bases and sites, advising people of the consensual and non-consensual identification and search regime and notifying that offences may apply for failing to comply with non-consensual identification and search requirements.

Notices should be worded as follows:

“You are about to enter Defence premises.

Unauthorised entry to these premises is an offence carrying a significant maximum monetary penalty (*Defence Act 1903* Part VIA, section 72P).

You may be asked to:

- provide identification or evidence of your authority to be on these premises; or
- undergo a search of your person or permit a search of things in your possession (including vehicle).

If you do not consent, you may be refused entry to these premises or, if already on the premises, denied free exit and detained on the premises.

Further, a SDSO may:

- require that you provide identification or evidence of your authority to be on the premises; or
- conduct a non-consensual search of your person and things in your possession (including vehicle).

It is an offence carrying a significant maximum monetary penalty if, while on the premises, you:

- fail to provide evidence of your identity and authority to be on these premises if required to do so by a SDSO (Defence Act 1903 Part VIA section 71V); or
- hinder or obstruct a SDSO from performing a non-consensual search of your person and things in your possession, including a vehicle (*Defence Act 1903* Part VIA, section 71W).

Defence Act 1903, Part VIA, Security of Defence Premises"

Note: *There are specific signage requirements applying to declared explosive ordnance depots[18].*

[18] For further information on declared explosive ordnance depot Refer to Annex G to DSPF Control 76.1 - *Special Search Provisions for Declared Explosive Ordnance Depots*.

Restrain and Detain Powers

110. Under Part VIA of the *Defence Act 1903* and this DSPF part, DSOs are authorised to restrain and detain people to support the enforcement of the identification, search and seizure regime. The power to restrain and detain a person is authorised in specific circumstances only and, under the *Defence Act 1903* Part VIA section 72J, is solely for the purposes of placing the person in a Federal, State or Territory police officer's custody at the earliest practicable time.

Note: *To restrain and detain a person does not necessarily require that they are physically restricted. A verbal direction that a person must remain on Defence premises until the arrival of police constitutes an exercise of the power to restrain and detain.*

111. The specific circumstances in which a DSO may restrain and detain a person are discussed in detail in the earlier sections of this DSPF part on Identification Powers and Search Powers. In summary, under the *Defence Act 1903* Part VIA, a DSO may restrain and detain a person if the person is on Defence premises and either:

a. refuses an identification request or requirement;

b. fails to provide evidence that satisfies the DSO in response to an identification request or requirement;

c. refuses a request for a consensual person or vehicle search;

d. hinders or obstructs a non-consensual person or vehicle search;

e. is an occupant in a vehicle and the person apparently in control of the vehicle refuses a consensual vehicle search;

f. is an occupant in a vehicle and a person hinders and obstructs a non-consensual search of the vehicle;

g. complies with a consensual or non-consensual identification or search action and, as a result, the DSO reasonably believes the person:

   i. is not authorised to be on the premises;

   ii. constitutes a threat to the safety of people on the premises; or

   iii. has or may commit a criminal offence on, or in relation to the premises; or

h. is an occupant in a vehicle and, as a result of a vehicle search, the DSO reasonably believes the vehicle or anything in it:

   i. is not authorised to be on the premises;

ii. constitutes a threat to the safety of people on the premises; or

iii. relates to a criminal offence that has or may be committed on, or in relation to the premises.

Note: *A DSO is not permitted to restrain and detain a person who has yet to enter a Defence base or site through the access control point that is located at the external perimeter of that base or site. If the circumstances detailed at sub-paragraphs b to h occur when a person is seeking to enter a Defence base or site through an access control point that is located at the external perimeter, the DSO is only authorised to refuse the person entry to the base or site. If a person who has been refused entry to Defence premises continues to loiter near the premises or causes some other disturbance, the police should be contacted to deal with the situation.*

112. A DSO should immediately contact the police in every instance where they have restrained and detained a person.

113. Under the *Defence Act 1903* Part VIA section 71T, if a SDSO reasonably believes that a person who has been restrained and detained constitutes a threat to safety of persons on Defence premises, they may conduct a non- consensual search of the person while awaiting the arrival of police.

114. In exercising the power to restrain and detain, a DSO, at all times and in all circumstances, is required to:

a. only use force against a person or item that is reasonable and necessary;

b. not subject a person to greater indignity than is reasonable and necessary; and

c. only restrain and detain for the purposes of placing the person in police custody at the earliest practicable time.

115. The power to restrain and detain a person is discretionary. A DSO must determine whether it is appropriate to restrain and detain a person in the circumstances described in this DSPF part “Restrain and Detain” in paragraph 117 having regard to:

a. the safety of the person, the DSO and other people on the premises;

b. the proximity of police assistance;

c. the seriousness of the circumstances giving rise to the exercise of the d. restrain and detain power;

d. the age and vulnerability of the person – for example trespassing teenagers would be handled differently to suspected terrorists;

e. whether the person is violent or their demeanor gives rise to the apprehension of violence;

f. the availability of suitable facilities to hold a person safely until the arrival of police; and

g. the SAFEBASE security alert level as this could be an indication of the potential seriousness of the circumstances.

116. Alternative response options must be assessed and implemented so as to minimise the use of force. When determining the most appropriate restrain/detain response, a DSO must also give consideration to:

a. the proximity of police assistance;

b. the age and vulnerability of the person;

c. the level of physical aggression presented by the person being restrained – for example, a person who is compliant to a request to wait in a particular location until the arrival of police would be handled differently to a person who is physically aggressive and confrontational towards the DSO;

d. whether the person is violent or their demeanor gives rise to the apprehension of violence;

e. whether the person has attempted, or is likely to attempt to flee;

f. whether the person is required to be escorted or detained with others;

g. the necessity to prevent the person from injuring themselves, or any other person;

h. the necessity to restrain the person to prevent the loss, concealment or destruction of evidence; and

i. whether the person has a weapon.

117. If the person has a weapon, the DSO must exercise caution for their own safety and the police must be contacted. Contracted Defence security guards and Defence security screening employees must not attempt to use force to restrain and detain an armed suspect. Security authorised Defence Force members, who have been trained to deal with armed suspects, may deal with the situation in accordance with their training.

Note: *Depending on the situation, the presence of a weapon could indicate that an attack on Defence premises is likely to result in death or serious injury is imminent. In these circumstances, security authorised Defence Force members may be able to exercise their powers in responding to an attack*[19]*.*

118. Only security authorised Defence Force members may use equipment (such as handcuffs) to restrain and detain a person if it is considered reasonable and necessary to do so. Security authorised Defence Force members must have been trained in the use of this equipment prior to its use.

119. A security authorised Defence Force member must not use handcuffs to restrain a minor unless they believe on reasonable grounds that the use of handcuffs is essential for the welfare or security of the minor or other people.

120. Security authorised Defence Force members may use military working dogs to assist the DSO to restrain or detain a person. For further information on the use of military working dogs under the identification, search and seizure regime, refer to paragraphs 103 to 105 within this DSPF part - "*Use of Military Working Dogs*".

Detention

121. A person, who is being detained while awaiting the arrival of police should, where practicable, be held in an area away from other people. Depending on the availability of suitable facilities, this could be in a potentially lockable room or private area located near the access control point. Where practicable, a person being temporarily detained should be kept under observation to avoid occurrences such as destruction of evidence or self-harm.

122. The dignity, safety and proper treatment of the person awaiting transfer to police custody is to be maintained at all times.

123. A DSO **must** provide a detained person an explanation for their apprehension.

124. A DSO is not to deny necessary medical treatment to a person who has been detained. If the injuries are of a serious nature, an ambulance must be called.

125. If a DSO subsequently determines that there is no longer a basis for detaining a person, the DSO should release the person.

126. It is recommended that the use of facilities to support detention should be determined on the basis of the available facilities at the site and the particular circumstances of the situation.

[19] For further information on Armed Security Wardens refer to DSPF Principle 83 – *SAFEBASE*.

Procedural Guidance

127. Contracted Defence security guards should comply with the restrain and detain response procedures detailed in their assignment instructions.

128. SDSO should comply with the restrain and detain response procedures applicable to their category of DSO as contained within the SOPs. The specific circumstances governing the appropriate use of handcuffs by security authorised Defence Force members should be included in the SOPs.

Reporting Requirements

Search Report

129. Contracted Defence security guards should maintain log books to record details of all consensual searches undertaken when no dangerous or prohibited items are found. At a minimum, this log book should include the following information:

a. the person's name;

b. the person's pass/ID number;

c. location of the search;

d. date and time of the search; and

e. the type of search (person/carried item/vehicle).

130. In situations where a dangerous or prohibited item is found, a DSO should prepare a report on the incident. This report must be signed by the DSO and include the following information:

a. the person's name;

b. the person's pass/ID number;

c. status of the person (Defence civilian/ADF member/contractor/visitor);

d. location of the search;

e. date and time of the search;

f. whether the search was consensual or non-consensual;

g. whether the person hindered or obstructed the search;

h. the type of search (person/vehicle/item);

i. if a vehicle has been searched, the vehicle registration, make and model; and

j. a description of the item(s) found.

131. The report must be signed by both DSOs present during the search and the person who has been searched. If the person refuses to sign, this should also be noted.

132. The discovery of a dangerous or prohibited item during a search also constitutes a security incident. Additional reporting requirements for security incidents will apply[20].

Restrain/Detain Report

133. When a DSO has restrained and detained a person, the official must also record the time the detention of the person commenced.

134. It is recommended that the restrain/detain report include information on any obvious injuries or medical concerns regarding the person being restrained and detained by the DSO and any treatment provided.

135. If a person has been detained and then released (i.e. if a DSO subsequently determines that there is no longer a basis for detaining a person), a report must still be prepared that provides information on the original reason for detention and the reason for release.

Use of Force Report

136. In all cases where a DSO uses force, he or she is to, as soon as is practicable, submit a report through the BSM/SADFO to the Head Defence Support Operations (HDSO) and the Chief Security Officer setting out the full details of the force used and the circumstances in which force was applied. This includes any situation where the DSO used force:

a. to conduct a non-consensual search of a person;

b. to break open an item in order to conduct a non-consensual search;

c. to restrain and detain a person;

d. to stop and detain a person; or

e. a military working dog was released against a person.

---

[20] For further information on reporting requirements refer to DSPF Principle 77 - *Security Incidents and Investigations*.

Note: *Separate reporting requirements exist for Armed Security Wardens who use force when exercising their powers.*

Roles and Responsibilities

Secretary

137. The Secretary is to approve the form of identity cards for the DSO in writing.

138. The Secretary is to issue an identity card to each DSO. The Secretary may delegate the authority to issue DSO identity cards in accordance with s 71E of *the Defence Act*.

139. A DSO is to return their identity card to the Secretary within seven days of ceasing to be a DSO. The Secretary may delegate the authority to receive DSO identity cards in accordance with *the Act*.[21]

Group Heads and Service Chiefs

140. Group Heads and Service Chiefs are responsible for guarding contracts that do not fall within Garrison Support activities managed by Defence Support and Reform Group[22].

First Assistant Secretary Service Delivery (FAS SD)

141. FAS SD is responsible to Deputy Secretary Estate and Infrastructure for the delivery of contracted guarding services to Defence bases covered in the Base Accountabilities Model[23].

Director General Estate Service Delivery (DG ESD)

142. DG ESD is responsible for determining, on the basis of advice from the SADFO and BSM, how the identification, search and seizure regime should be implemented at each Defence base.

---

[21] For further information on security official identity cards refer to Annex F to DSPF Control 76.1 - *Defence Security Official Identity Cards (DSOIC)*.

[22] For further information on contracted security guards refer to DSPF Principle 75 - *Contracted Security Guards*.

[23] For further information on contracted security guards refer to DSPF Principle 75 - *Contracted Security Guards*.

Base Support Manager (BSM) and Senior ADF Officer (SADFO)

143. The BSM and the SADFO, in consultation with Heads of Resident Units and as part of the base security plan development process, are to recommend to the DG ESD how the identification, search and seizure regime should be implemented at their base.

Base Support Managers

144. The BSM is responsible for coordination of whole-of-base security at SAFEBASE ALPHA, BRAVO and CHARLIE and for managing a response to a security incident at the Defence premise that requires routine coordination of the DSO or other base personnel and resources. The BSM is also accountable to the HDSO and the SADFO for the delivery of guarding services to meet the base security requirements[24].

Senior ADF Officer

145. The SADFO supports the BSM in the planning of the identification, search and seizure regime and its implementation at SAFEBASE ALPHA, BRAVO and CHARLIE. In addition, each SADFO has particular responsibilities associated with the assumption of command at SAFEBASE DELTA and ECHO, and for commanding the response to a security incident that requires a capability beyond that routinely available and that involves ADF members[25].

Commanders and Managers

146. If guarding services are not an element of base support services, the relevant Commander or Manager is responsible for recommending to the BSM and SADFO, based on a security risk assessment, the guarding requirements for their base[26].

Contract Managers

147. Contract managers are responsible for ensuring that contracts for guarding services meet the identified guarding requirements and for the development of assignment instructions for contracted guards[27].

---

[24] For further information on contracted security guards refer to DSPF Principle 75 - *Contracted Security Guards*.

[25] For further information on SAFEBASE level and command refer to DSPF Principle 83 – *SAFEBASE*.

[26] For further information on contracted security guards refer to DSPF Principle 75 - *Contracted Security Guards*.

Outsourced Service Providers of Security Services

148. Outsourced service providers of security services are responsible for the implementation of assignment instructions for guarding services.

Key Definitions

149. **Assignment Instructions**. An operational document detailing the specific duties to be performed under a contract for guarding and patrolling services (Australian Standard (AS) 4421).

150. **Consensual search**. A consensual search of a person has the same meaning as a limited search of a person as defined by the *Defence Act 1903* section 71A. Refer to the definition of a limited search below. A consensual search of a vehicle refers to a search of a vehicle, or anything in the vehicle, that is undertaken with the consent of the person apparently in control of the vehicle. A thing includes substances or things in magnetic or electronic form.

151. **Contracted Defence security guard**. A category of Defence Security Official. Refer paragraph 156 for further information.

152. **Declared explosive ordnance depot**. A specified area of land or any other place, building or structure identified and authorised by the Minister as a 'declared explosive ordnance depot'. Declared explosive ordnance depots are further defined in the *Defence Act 1903* Part VIA in section 71L.

153. **Defence Access control point**. Defined by the *Defence Act 1903* Part VIA in section 71A as a point of entry to, or exit from Defence premises or a part of Defence premises, where entry or exit is controlled or limited by any means. In addition to being located at the perimeter, Defence access control points may be also situated at specified locations within the premises. A Defence access control point may also be established at the base of a gangway to a vessel, the stairs leading up to an aircraft or a ramp providing access to a vehicle. Further explanation of Defence access control points is provided at Annex C to DSPF Control 76.1 – *Defence Access Control Points*. In this DSPF part, Defence access control points are referred to as access control points.

154. **Defence accommodation**. Defined in the *Defence Act 1903* Part VIA section 71A as any building, structure, or place within Australia that is used for, or in connection with, the accommodation of a group of members of any part of the Defence Force. It includes accommodation blocks and complexes accommodating

---

[27] For further information on contracted security guards refer to DSPF Principle 75 - *Contracted Security Guards*.

members of the Defence Force and their families, but does not include single, stand-alone residences, which are located off base and are either privately owned or rented by Defence Force members. Defence accommodation includes areas connected with accommodation buildings such as private car parks, gardens and recreational facilities which form part of the accommodation buildings.

155. **Defence premises**. Defined in section the *Defence Act 1903* Part VIA 71A as any area of land or other place, a building or other structure, a vehicle, vessel or aircraft, or a prohibited area within the meaning of the *Defence (Special Undertakings) Act 1952* that is located in Australia and is owned or occupied by the Commonwealth for use by the Defence Force or the Department. It includes any fixed or moveable ramp, stairs or other means of access to or from a vehicle, vessel or aircraft.

Note: *Land or buildings that have a Defence purpose, that are not currently in use by the Defence Force or the Department, do not meet the legal definition of Defence premises for the purposes of the identification, search and seizure regime. For example, a former Defence base or a portion of an operational Defence base that has been set aside for a use that is unrelated to the Defence Force or the Department, is not regarded as Defence premises and therefore the identification, search and seizure regime does not apply to these locations.*

Note: *A Defence base, as defined and referred to in other parts of the DSPF, falls within the definition of a Defence premise.*

156. **Defence Security Official (DSO).** Defined in the *Defence Act 1903* Part VIA section 71A as a contracted Defence security guard, a security authorised member of the Defence Force or a Defence security screening employee. DSOs are authorised by the Minister to exercise identification, search, seizure and related powers under Part VIA of the Act.

157. **Defence security screening employee**. A category of DSO. For further information refer to paragraphs 11 to 14 within this DSPF part - "*Defence Security Screening Employees*", and Table 1 – "*Categories of Defence Security Officials*" within DSPF Control 76.1.

158. **Detain**. To deny a person free exit from Defence premises until the arrival of police. Section 71Y of the Act also provides that a SDSO may stop and detain a person, or vehicle, vessel or aircraft to:

a. require a person to provide evidence of particular matters; or

b. search the person, vehicle, vessel or aircraft.

159. **Identification and Search Warden (ISW).** A specialised sub-category of security authorised members of the Defence Force (for further information refer to the Key Definitions section within the DSPF Principle, and Table 1 – "*Categories of Defence Security Officials*" within DSPF Control 76.1 further information) who are

authorised by the Minister to affect the identification, search and seizure regime contained in Part VIA of the *Defence Act 1903*.

160. **Limited search**. A limited search of a person is defined in the *Defence Act 1903* Part VIA section 71A. It is a search of a person that is performed by a DSO with the person's consent and includes:

a. a search of items in the possession of a person that may include requesting the person to remove his or her overcoat, coat or jacket and any gloves, shoes and hat and an examination of any of those items that the person consents to remove; or

b. a search of a person conducted by quickly running the hands over the person's outer garments and an examination of anything worn or carried by the person that is conveniently and voluntarily removed by the person.

A limited search does not include requesting the person remove all of their garments.

Any reference to a consensual search of a person in this DSPF part means a limited search of a person undertaken with the person's consent.

161. **Minor**. A person who has not attained the age of 18 years.

162. **Non-consensual search**. A non-consensual search of a person has the same meaning as a search as defined by section 51 of the Act. It is performed by the SDSO without the requirement for consent from the person. Refer below for the definition of a search. A non-consensual search of a vehicle refers to a search of a vehicle, or anything in the vehicle, that is performed by the SDSO without the requirement for consent from the person apparently in control of the vehicle. A thing includes substances or things in magnetic or electronic form.

163. **Person**. In this DSPF part, a reference to a person includes a Defence APS employee, a Defence Force member, a Defence contractor or a visitor.

164. **Police**. In this DSPF part, a reference to police includes State and Territory Police Officers, AFP Officers and Protective Service Officers of the AFP.

165. **Restrain**. Any word or action that is used for the purpose or intent of restricting the free movement of another person.

166. **Search**. A search of a person has the same meaning as in section 51 of the *Defence Act 1903*. A search of a person is a search that is undertaken by a SDSO without the requirement for consent from the person and includes:

a. a search of a person or items in the possession of a person that may include requiring the person to remove his or her overcoat, coat, jacket, gloves, shoes and hat and an examination of those items; or

b. a search of a person conducted by quickly running the hands over the person's outer garments and an examination of anything worn or carried by the person that is conveniently and voluntarily removed by the person.

A search of a person differs from a limited search of a person in that the 'pat down' of the person can be conducted after requiring the removal of the person's overcoat, coat, jacket, gloves, shoes and hat.

A search of a person does not include requiring the person to remove all of their garments or an examination of the person's body cavities.

A search of a vehicle, as defined in the *Defence Act 1903* Part VIA section 71A, includes a search of a thing in the vehicle.

167. **Security authorised Defence Force member**. A category of DSO. For further information refer to paragraphs 15 to 17 of this DSPF part and Table 1 – "*Categories of Defence Security Officials*" within DSPF Control 76.1.

168. **Special Defence Security Official (SDSO).** A security authorised member of the Defence Force or a Defence security screening employee as defined by the *Defence Act 1903* Part VIA sections 71C and 71D. SDSO are authorised under the *Defence Act 1903* Part VIA to undertake non-consensual identification, search, seizure and related actions.

169. **Vehicle**. In this DSPF part, a reference to a vehicle includes a vessel and an aircraft.

Further Definitions

170. Further definitions for common DSPF terms can be found in the Glossary.

171. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – *Other Non-Statutory Search Regimes*

Annex B – *Offences and Penalties*

Annex C – *Defence Access Control Points*

Annex D – *Defence Security Officials – Training and Qualification Requirements*

Annex E – *Summary of Defence Security Officials' Powers*

Annex F – *Defence Security Official Identity Cards (DSOIC)*

Annex G – *Special Search Provisions for Declared Explosive Ordnance Depots*

Document Administration

Identification

DSPF control	Identification, Search and Seizure Regime
Control Owner	DG ESD
DSPF number	76
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry

Related Information

General Principle and Expected Outcomes	Identification, Search and Seizure Regime
Government compliance	**PSPF Core Requirements:** Agency physical security policy and planning; protection of employees **Legislation:** *Defence Act 1903*, *Part VIA, Security of Defence Premises*.
Read in conjunction with	Access Control
See also DSPF	Physical Security Certification and Accreditation Security Incidents and Investigations
Implementation Notes, Resources and Tools	The scope of this principle and underlying security controls is confined to describing the identification search and seizure regime and does not describe the role of Armed Security Wardens or the operation of the Enhanced Self Defence Capability. Australian Government physical security management protocol

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	DG ESD	Launch

Defence Security Principles Framework (DSPF)

Annex A to Identification, Search and Seizure Regime – Other Non-Statutory Search Regimes

Other Non-Statutory Search Regimes

1. At Defence sites that are assessed as having a low security risk and where there are minimal assets requiring protection, it may be determined that implementation of the statutory search regime contained within the *Defence Act 1903* (the Act), Part VIA, Security of Defence Premises is not warranted. At these sites, security searches that are based on common law can be conducted by appropriately trained contracted security guards in accordance with the policy contained in this Annex and approved base security plans and instructions.

2. At Defence sites that are not operating the statutory search regime contained in the Act, security inspections are strictly limited to:

a. consensual inspections of carried items, or items in a person's possession on entry to and exit from the site; and

b. consensual inspections of vehicles, including things in the vehicle, on entry to and exit from the site.

3. A search of a person that involves a 'pat down' over the person's outer garments and non- consensual searches are not to be conducted under any circumstances.

4. All inspections are to be conducted in accordance with approved base security plans and instructions. Refer to DSPF Principle 83 - *SAFEBASE* for further information. Additionally, all contracted security guards who conduct inspections are to meet the security, licensing and competency requirements detailed in DSPF Principle 75 - *Contracted Security Guards*.

Non-statutory Consensual Inspection of Carried Items or Vehicle on Entry to or Exit from a Defence Base

5. Contracted security guards may request a person, who is about to enter or exit a Defence site, to permit a consensual inspection of their carried items or items in their possession.

6. Similarly, contracted security guards may request a person apparently in control of a vehicle that is about to enter or exit a Defence site to permit a consensual inspection of the vehicle, including things in the vehicle.

Inspection Process

7. During a non-statutory consensual inspection, a person is to display all items and their identification as requested by contracted security guards. This may involve removing items from vehicles.

8. The contents of briefcases used for carrying classified material are not exempt from a non-statutory consensual inspection. If consent is given to undertake an inspection then:

a. the briefcase may be opened and the contents given a cursory inspection to verify the existence of documented authorisation to carry the material and to ensure that the material has been properly protected and does not appear to have been subject to tampering; and

b. the person carrying the briefcase can be asked to move papers and files around, but files are not to be opened.

9. Where practicable, storage facilities should be made available outside the Defence base to allow personnel to securely store items prior to entry.

10. Two contracted security guards should be present at all non-statutory consensual inspections to avoid any evidential dispute. The guards are to be appropriately trained in the conduct of inspections. In order to protect the privacy of the person, guards must not record or discuss anything of a private or personal nature observed during the conduct of a non-statutory consensual inspection.

11. Same gender non-statutory consensual inspections may not always be possible. Females or males who are uncomfortable with having their vehicles or carried items inspected by a guard of the opposite gender may choose to have another person (a colleague for example) present during the inspection. That person must be able to attend the site in a timely manner.

12. Contracted guards are to conduct non-statutory consensual inspections in accordance with the Standard Operating Procedures (SOPs) held by Defence Estate and Infrastructure Group. These SOPs must be referred to in any guarding contract that includes non-statutory consensual inspections.

13. If a dangerous or prohibited item is located during a non-statutory consensual inspection and the person in possession of it has no reasonable explanation or authority for having the item then the person is not to enter the base with the item.

14. Form *AD432 – Security Inspection Report* is to be completed if a dangerous or prohibited item is found, or if a person complains about the manner in which the non-statutory consensual inspection was undertaken. As a completed Form AD432 may be used as evidence, it is to be signed by the person as a true and accurate record of events, or provide an explanation as to why the individual failed to sign the report.

15. Completed reports are to be forwarded in a timely manner through the chain of command to the Commander or Manager. If the report is a complaint about the manner in which the non-statutory consensual inspection was undertaken, the Commander or Manager is to undertake a review of the conduct of the inspection.

Refusal to Consent to a Non-statutory Inspection

16. **Visitors**. A visitor may be denied access to a Defence base if they refuse to consent to a non-statutory inspection of their carried items or vehicle on entry. A visitor must not be denied exit from a Defence base if they refuse to consent to a non-statutory inspection on exit.

17. **Defence Personnel**. Defence personnel must not be denied entry to, or exit from a Defence base if they refuse to consent to a non-statutory inspection of their vehicle or carried items. In the event that a Defence Force member or civilian employee of the Department of Defence refuses to consent to a non-statutory inspection of their carried items or vehicle, their immediate supervisor **must** be informed. Repeated refusals may lead to disciplinary action under the *Public Service Act 1999* (for not complying with a lawful and reasonable direction) or the *Defence Force Discipline Act 1982* (for refusing to comply with the security requirements of the DSPF).

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Other Non-Statutory Search Regimes
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	76.1

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	DG ESD	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B to Identification, Search and Seizure Regime – Offences and Penalties

Offences and Penalties

1. The *Defence Act 1903* (the Act) Part VIA establishes offences and penalties associated with the execution of the identification, search and seizure regime.

Unauthorised Entry on Defence Premises or Defence Accommodation

2. Under *the Act* Part VIA section 72P, a person commits an offence if they enter, or are on Defence premises or in Defence accommodation when they are not authorised to do so.

3. A member of the Defence Force, Australian Federal Police, State and Territory police, or a protective service officer may, without a warrant, arrest the person if the member reasonably believes that the person is not authorised to be on the Defence premises or in the Defence accommodation. In the event that a person is arrested by a Defence Force member, the person is to be placed in police custody as soon as practicable after the arrest.

Note: *A person arrested by a Defence Force member in the situation outlined above cannot be transferred to the custody of a Protective Service Officer of the Australian Federal Police.*

Note: *This offence is also a protective service offence for the purposes of the Australian Federal Police Act 1979.*

4. Only members of the Defence Force who have been appropriately trained and equipped may arrest a person in the circumstances outlined above.

5. A member of the Defence Force may use handcuffs, if it is considered reasonable and necessary, to restrain a person following their arrest on Defence premises or in Defence accommodation. Only members of the Defence Force who have been properly trained and equipped may arrest a person in the circumstances outlined above.

Note: *Authorised Commonwealth Officers have comparable powers to apprehend and detain a person who has trespassed on prohibited Commonwealth land or discharged a firearm on or over Commonwealth land. The exercise of these powers is separate from the powers of a Defence Security Official (DSO) as specified in Part VIA of the Act.*

Refusal to Provide Evidence of Identity in Response to a Non-Consensual Identification Action

6. Under the Act Part VIA section 71V a person, who is on Defence premises, commits an offence if a Special Defence Security Official (SDSO) requires the person to provide evidence of their identity or authority to be on the premises, and the person:

a. refuses;

b. fails to provide the evidence; or

c. gives a name or address that is false in a material particular.

7. A monetary penalty applies to this offence.

8. The offence, however, will not apply if the SDSO did not comply with the requirement to produce their identity card and inform the person of the effect of refusing to comply with the requirement, prior to exercising this power.

Note: *This offence is also a protective service offence for the purposes of the Australian Federal Police Act 1979.*

Offences Relating to Consensual Search Powers

9. Under the Act Part VIA section 71Q, a DSO commits an offence if they conduct a limited search of person without the person's consent. A monetary penalty applies to this offence.

10. Further, a DSO commits an offence if they conduct a search of a vehicle, purportedly under the consensual regime, and the person apparently in control of the vehicle did not consent to the search. A monetary penalty applies to this offence.

11. These offences would apply in circumstances where the person believed they had to comply with the consensual search request. That is, a DSO **must not** do anything that causes a person to believe they must submit to a consensual search. A person must freely and voluntarily provide clear consent to the DSO immediately prior to the conduct of any consensual search.

12. A DSO **must** immediately cease a consensual limited search of a person or a consensual search of a vehicle if the person subsequently withdraws their consent. A DSO commits an offence if they continue to undertake a purportedly consensual search after consent has been withdrawn.

Hindering or Obstructing a Non-Consensual Search by a Special Defence Security Official

13. Under *the Act* Part VIA section 71W, a person commits an offence if they hinder or obstruct a non-consensual search by a SDSO. The offence only applies if prior to conducting the non-consensual search, the official produced their identity card for inspection and informed the person of the consequences of refusing to comply with, or hindering the non-consensual search. A monetary penalty applies to the offence.

Note: *If an SDSO reasonably believes that a person constitutes a threat to safety such that complying with the requirement, prior to conducting a non-consensual search, places the safety of the official and others at risk, they may temporarily delay presenting their identity card. For example, this might occur if the official reasonably believes the person is carrying a concealed weapon. In these circumstances, after the immediate threat to safety has been resolved, the official is required to produce his or her identity card for inspection by the person and inform the person of the effect of hindering or obstructing the search.*

Note: *This offence is also a protective service offence for the purposes of the Australian Federal Police Act 1979.*

Return of Defence Security Official Identity Cards

14. Under the Act Part VIA section 71E, a person commits an offence if they do not return their identity card to the Secretary (or delegate) within 7 days of ceasing to be a DSO. A monetary penalty applies to this offence. For further information, refer to Card Return in Annex F to DSPF Control 76.1 - *Defence Security Official Identity Cards (DSOIC)*.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Offences and Penalties
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	76.1

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	DG ESD	Launch

Defence Security Principles Framework (DSPF)

Annex C to Identification, Search and Seizure Regime – Defence Access Control Points

Defence Access Control Points

1. A Defence access control point is an identified location on a Defence premises where Defence Security Officials (DSOs) are authorised to exercise their identification, search and related powers.

2. A Defence access control point is defined by the *Defence Act 1903* Part VIA section 71A as a point of entry to, or exit from Defence premises or a part of Defence premises, where entry or exit is controlled or limited by any means. In addition to being located at the perimeter, Defence access control points may be also situated at specified locations within the premises. A Defence access control point may also be established at the base of a gangway to a vessel, the stairs leading up to an aircraft or a ramp providing access to a vehicle. In this annex, Defence access control points are referred to as access control points.

3. A sign or boundary marker on its own does not constitute an access control point. An access control point must include one or more measures to limit access. These measures may include, but are not limited to:

a. the presence of a DSO;

b. the requirement to present access cards or other identification for inspection;

c. electronic security barriers fitted with access card readers;

d. electronic handheld access card readers; or

e. retinal scanners, hand scanners and comparable devices or other biometric identity management solutions.

4. These measures may be used in conjunction with, but are not limited to, any of the following physical security controls:

a. gates, including boom gates;

b. security bollards;

c. locked or electronically controlled doors; or

d. entry points to vehicles, vessels or aircrafts including gangways and stairs.

5. An access control point could be set up at the entrance to an outsourced service provider's facility if it is located on Commonwealth land or within a building occupied by the Commonwealth.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Defence Access Control Points
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	76.1

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	DG ESD	Launch

Defence Security Principles Framework (DSPF)

Annex D to Identification, Search and Seizure Regime – Training and Qualification Requirements

Defence Security Officials – Training and Qualification Requirements

1. Training and qualification requirements are outlined in two Legislative Instruments:

a. Defence (Contracted Defence Security Guards – Training and Qualification Requirements) Determination 2013, dated 1 September 2013; and

b. Defence (Security Authorised Members - Training and Qualification Requirements) Determination 2013, dated 25 September 2013.

2. This Annex outlines these requirements against different roles.

Contracted Security Guards

3. Refer to DSPF Principle 75 – *Contracted Security Guards* for more detailed information.

Qualifications

4. The person **must** hold:

a. a current certificate II in Security Operations or a higher qualification in Security Operations; or

b. in the case of guards carrying out specialist functions, a Certificate III in Security Operations and/or additional competencies.

5. The person **must** hold a current licence to work as a security guard in the State or Territory where the person works, or would work, as a contracted defence security guard.

Training

6. Contracted security guards are to complete a Defence-endorsed training package (delivered by the contracted security guard service provider, or Defence). This is to cover topics such as:

a. Defence security policy and relevant Federal, State and Territory laws;

b. Defence protocols (including rank structure, customer service, etc.);

c. the Defence security environment;

d. Defence policing; and

e. the SAFEBASE alert level security system.

7. For each year after the person complete training to refresh or update the skills and knowledge the person needs to perform the duties of a contracted defence security guard.

8. The person **must** hold a current qualification or competency in first aid.

9. The person **must** hold, at minimum, a current Baseline security clearance issued or recognised in accordance with the Department's security policy. A higher clearance may be required for specialist tasks.

10. The person **must** have completed the course Defence Security Official – Roles and Responsibilities – Course Campus ID 00007028.

Defence Security Screening Employee

11. Defence Security Officials (DSOs) who are Defence Australian Public Service security screening employees are required to have fulfilled the training, qualification, probity and licensing prerequisites as determined by the Minister, or his delegate, in a legislative instrument.

12. A valid first aid qualification is a mandatory requirement for security screening employees, to administer qualified basic first aid as required.

13. Security screening employees must hold a minimum Defence security clearance.

14. Security screening employees **must** have completed the course Defence Security Official – Roles and Responsibilities – Course Campus ID 00007028.

Security Authorised Defence Force Members

Identification and Search Warden

15. DSOs who are Security Authorised Defence Force Members **must** have fulfilled the training, qualification, probity and licensing prerequisites as determined by the Minister, or his delegate, in a legislative instrument (Defence (Security Authorised Members-Identification and Search Wardens: Training and Qualification Requirements) Determination 2014, dated 27 November 2014).

Qualifications

16. The training and qualification requirements for a person to be a Security Authorised Member of the Defence Force—Identification and Search Warden are:

17. The person **must** have successfully completed:

a. the Service Police Officer Basic Course;

b. the Service Police Basic Course; or

c. training that is of a kind approved, in writing, by the Minister, or a delegate of the Minister, and that is designed to give the person competence in the following:

(1) managing security risk situations;

(2) searching people, vehicles and other things;

(3) controlling access to and exit from premises;

(4) conducting search and seizure operations; and

(5) operational safety skills and tactics.

Training

18. The person **must** have successfully completed training that is:

a. of a kind approved, in writing, by the Minister or a delegate of the Minister; and

b. designed to give the person familiarity with the following:

(1) The Act and other relevant Commonwealth, State and Territory laws;

(2) the security policies and protocols of the Department;

(3) other matters relevant to the security of the Department;

(4) the policing arrangements used by the Defence Force; and

(5) the security alert system used by the Department.

19. Every 12 months after the person has successfully completed both the course or training outlined in paragraphs 15 and 17 of this Annex, the person must successfully complete training that is:

a. of a kind approved, in writing, by the Minister or a delegate of the Minister; and

b. designed to refresh or update the skills and knowledge the person needs to perform the duties of a Security Authorised Member of the Defence Force – Identification and Search Warden.

20. The person **must** hold a current security clearance issued or recognised in accordance with the Department's security policy.

Military Working Dog Handler

Military Dog Handler

21. DSOs who are Security Authorised Defence Force Members are required to have fulfilled the training, qualification, probity and licensing prerequisites as determined by the Minister, or his delegate, in a legislative instrument (Defence (Security Authorised Members – Military Working Dog Handlers: Training and Qualification Requirements) Determination 2015, dated 2 November 2015).

22. Military dog handlers are required to undertake the training below, where relevant:

23. Successfully complete:

a. the Air Force Security Military Working Dog Handler 1 course; or

b. the Air Force Security Military Working Dog Handler Reteam course; and

c. while working with his or her assigned dog as a Military Working Dog team, have been assessed by the Manager of the Military Working Dog section in the Air Force as proficient at the operational level of capability.

24. If the person is assigned an Explosive Detector Dog, the person must have successfully completed;

a. the Australian Customs Service Explosive Detector Dog course;

b. the United States Air Force Specialised Search Dog course; or

c. the Royal Australian Air Force Explosive Detector Dog course.

25. Every 12 months Military Dog Handlers are to undertake the following:

a. the Air Force Security Military Dog Handler 1 course; or

b. the Reteam course is to be completed and assessed as being proficient at the operational level of capability.

26. Every 12 months if a Military Dog Handler is also an Explosive Detector Dog Handler they must undertake and successfully complete one of the following:

a. the Australian Customs Service Explosive Detector Dog course;

b. the United States Air Force Specialised Search Dog course; or

c. the Royal Australian Air Force Explosive Detector Dog course.

27. The person must successfully complete all training that is:

a. of a kind approved, in writing, by the Minister or delegate of the Minister, and

b. designed to refresh or update the skills and knowledge the person needs to perform the duties of a Security Authorised Member of the Defence Force – Military Working Dog Handler.

28. A requirement to undertake the training and to be a Security Authorised Member of the Defence force, a valid security clearance is to be held in accordance with the Departments security policy.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Training and Qualification Requirements
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	76.1

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	DG ESD	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex E to Identification, Search and Seizure Regime – Summary of Defence Security Officials' Powers

Summary of Defence Security Official's Powers

Table 1 – Summary of Defence Security Officials' Powers

Power	*Defence Act 1903* Reference	Defence Contracted Security Guard	Defence Security Screening Employee	Security Authorised Defence ADF Member
Consensual identification and limited search of person about to pass an access control point including, in defined circumstances, authority to: • refuse to allow the person to pass the access control point; and • if on Defence premises, restrain and detain.	71H	Y	Y	Y
Consensual search of vehicle, vessel or aircraft at an access control point including, in defined circumstances, authority to: • refuse to allow the vehicle to pass the access control point; and • if on Defence premises, restrain and detain any people in the vehicle.	71J	Y	Y	Y

Power	*Defence Act 1903* Reference	Defence Contracted Security Guard	Defence Security Screening Employee	Security Authorised Defence ADF Member
Consensual identification of person on Defence premises if there is a reasonable belief the person is not authorised to be on the premises including, in defined circumstances, authority to: • restrain and detain.	71K	Y	Y	Y
Consensual limited search of person on a *declared explosive ordnance depot* including, in defined circumstances, authority to: • restrain and detain.	71M	Y	N/A	N/A
Consensual search of vehicle, vessel or aircraft while on a *declared explosive ordnance depot* including, in defined circumstances, authority to: • restrain and detain any people in the vehicle.	71N	Y	N/A	N/A
Non-consensual search of vehicle, vessel or aircraft at an access control point including, in defined circumstances, authority to: • refuse to allow a vehicle to pass an access control point; and • if on Defence premises, restrain and detain any people in the vehicle.	71S	N	N	Y

Power	*Defence Act 1903* Reference	Defence Contracted Security Guard	Defence Security Screening Employee	Security Authorised Defence ADF Member
Non-consensual identification and search of person on Defence premises if there is reasonable belief that person is not authorised to be on the premises, poses a threat to safety or may be involved in a criminal offence, including in defined circumstances, authority to:				
• request the person to leave and, if he/she refuses, remove the person from the premises; or	71T	N	N	Y
• in specific circumstances (safety of self and others) restrain and detain for purposes of placing them in custody of the police;	71T	Y	Y	Y
• If the ADF Special Defence Security Official (SDSO) is not available or it is not practical for them to undertake the search, the above duties can be undertaken.	71T	N	Y	Y

Power	*Defence Act 1903* Reference	Defence Contracted Security Guard	Defence Security Screening Employee	Security Authorised Defence ADF Member
Non-consensual search of vehicle, vessel or aircraft while on a Defence premises if there is reasonable belief that it is not authorised to be on the premises, constitutes a threat to safety or may be involved in a criminal offence, including authority to:				
• restrain and detain any people in the vehicle;	71U	N	N	Y
• If the ADF SDSO is not available or it is not practical for them to undertake the search, the above duties can be undertaken.	71U	N	N	Y
• If the ADF Special Defence Security Official (SDSO) is not available or it is not practical for them to undertake the search, the above duties can be undertaken.	71U	N	Y	Y
Stop and detain person, vehicle, vessel or aircraft, for the purposes of undertaking non-consensual identification or search actions • If the ADF SDSO is not available or its not practical for them to undertake the search, the above duties can be undertaken	71Y	N	N	Y

Power	*Defence Act 1903* Reference	Defence Contracted Security Guard	Defence Security Screening Employee	Security Authorised Defence ADF Member
Seize an item found on a Defence base or as a result of a search, if there is reasonable belief that it constitutes a threat to safety, or relates to a criminal offence, including authority to:				
• take such action that is reasonable and necessary to make the item safe or prevent it being used.	72	N	N	Y
• request the item to remain in place until the police arrive.	72	Y	Y	Y
Restrain and detain for the purpose of placing the person, at the earliest practicable time, into police custody.				
• Undertake common law (Citizens) arrest	72J	Y	Y	Y
• Use reasonable force to restrain and detain	72J	N	N	Y
Use equipment to examine items, including electronic equipment as part of the search process, or if the item constitutes a threat to safety or relates to a criminal offence. This includes using equipment to access data stored on an item. Staff who are qualified to utilise the equipment can only operate the equipment this may be on behalf of the DSO and SDSO	72E	Y	Y	Y

Power	*Defence Act 1903* Reference	Defence Contracted Security Guard	Defence Security Screening Employee	Security Authorised Defence ADF Member
Power to move certain unattended things to another place if it is necessary or desirable to do so	72F	Y	Y	Y
Use of dogs is limited to security authorised members of the Defence Force to assist in exercising their powers of search, restrain/detain and remove when it is considered reasonable and necessary	72M	N	N	Y

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Summary of Defence Security Officials' Powers
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	76.1

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	DG ESD	Launch

Defence Security Principles Framework (DSPF)

Annex F to Identification, Search and Seizure Regime – Defence Security Official Identity Card Delegations

Defence Security Official Identity Cards (DSOIC)

1. Under the *Defence Act 1903* (*the Act*) Part VIA, section 71E, all Defence Security Officials (DSO) **must** carry their identity cards at all times when performing the functions or exercising powers under Part VIA of the Act. In addition, under the Act Part VIA, section 72B a DSO **must** produce this card for inspection by a person before:

a. requesting or requiring the person to provide evidence of their identification or authority to pass an access control point or be on Defence premises;

b. requesting a consensual limited search of a person (including items in the person's possession) or a consensual search of a vehicle apparently under the person's control;

c. requiring a non-consensual search of the person (including items in the person's possession) or a vehicle apparently under the person's control; or

d. restraining, detaining or removing a person from Defence premises.

Card Issue

2. Under the Act Part VIA, section 71E (1), the Secretary **must** issue an identity card to each DSO. The Secretary may delegate the authority to issue DSO identity cards in accordance with the Act Part VIA, section 71G. In the event that this power is delegated, the Secretary **must** delegate the authority to issue DSOIC to specific Australian Public Service (APS) employees in Executive Level 2 positions or higher, or military officers holding the rank of Colonel (or equivalent) or higher. Delegates who have been authorised to issue DSOIC are listed in Appendix 1 to Annex F to DSPF Control 76.1 - *Defence Security Official Identity Card Delegations*.

3. Delegates are to be satisfied that the proposed DSO:

a. has met the relevant minimum training and qualification requirements as identified by the Minister in a legislative instrument; and

b. has met any other pre-conditions established in the ministerial authorisation for the relevant category or sub-category of DSO.

4. Every person issued with a DSOIC is to sign a form acknowledging that they:

a. may only use the card for the purpose of fulfilling their duties as a DSO; and

b. **must** return their identity card to a nominated point of contact within seven days of ceasing to be a DSO.

Card Return

5. Under the Act Part VIA, section 71E, a DSO **must** return their identity card to the Secretary within seven days of ceasing to be a DSO. A DSO commits an offence if they do not return their DSOIC within this timeframe. This offence does not apply if the card was lost or destroyed.

6. The Secretary may delegate the authority to receive DSOIC in accordance with the Act Part VIA, section 71G of. In the event that this power is delegated, the Secretary **must** delegate the authority to receive returned identity cards to specific APS employees at the APS 5 level or higher, and military officers of the rank of Captain (or equivalent) or higher. Delegates who have been authorised to receive DSOIC are listed in Appendix 1 to Annex F to DSPF Control 76.1 - *Defence Security Official Identity Card Delegations*.

7. Delegates who have received cards are to return the DSOIC to a pass office by SAFEHAND or destroyed on-site using an approved method and the pass office notified accordingly.

Format

8. Under the Act Part VIA, section 71E, the Secretary is to approve the format of the DSOIC in writing. The DSOIC should include a recent photographic image of the official. In accordance with the Secretary's direction, the DSOIC should also include:

a. the official's first name and surname;

b. an expiry period of five (5) years for DSOIC from the date of issue for the particular category or sub-category of Special Defence Security Official (SDSO); and

c. for security authorised Defence Force members, their rank.

9. Legal disclaimers appear on the reverse of the card to remind the bearer of the offence for not returning a DSOIC within 7 days and provide further instruction on how to return it.

10. Two forms of DSOIC have been developed to distinguish between officials who are authorised under the Act to exercise consensual powers only, and officials who are authorised to exercise both consensual and non-consensual powers.

a. Officials who are authorised to exercise consensual powers only will be identified through the use of an identity card that has 'Defence Security Official' printed in white font on a black background; and

b. Officials who are authorised to exercise both consensual and non-consensual powers will be identified through the use of a card that has 'Special Defence Security Official' printed in red font on a black background.

11. The distinction between DSOs and SDSOs supports proposed signage at primary access points that informs Defence employees and visitors of the exercise of consensual and non-consensual powers on the Defence premises. There is no requirement for a separate DSOIC to identify each discrete category or sub-category of Defence security official.

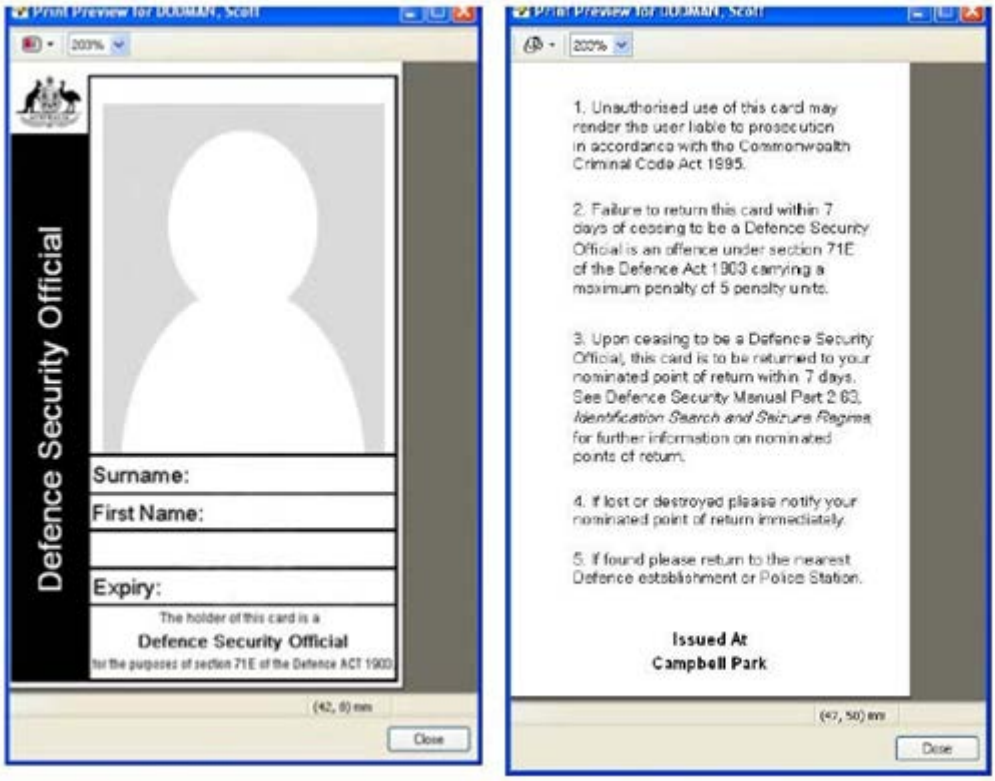
12. Training regimes require DSOs undertake refresher training within a specified timeframe in order to remain an official. In recognition of this safeguard, an expiration date is displayed on the front of the card that is linked to the date when the official is required to undertake refresher training. For further information on training requirements for DSOs refer to Annex D to DSPF Control 76.1 - *Defence Security Officials – Training and Qualification Requirements*.

13. As the Act also includes an offence relating to the failure to return a DSOIC within seven days of ceasing to be a DSO, legal disclaimers appear on the reverse of the card to remind the bearer of this offence and to provide instruction on how to return the card.

14. The DSOIC are reproduced below.

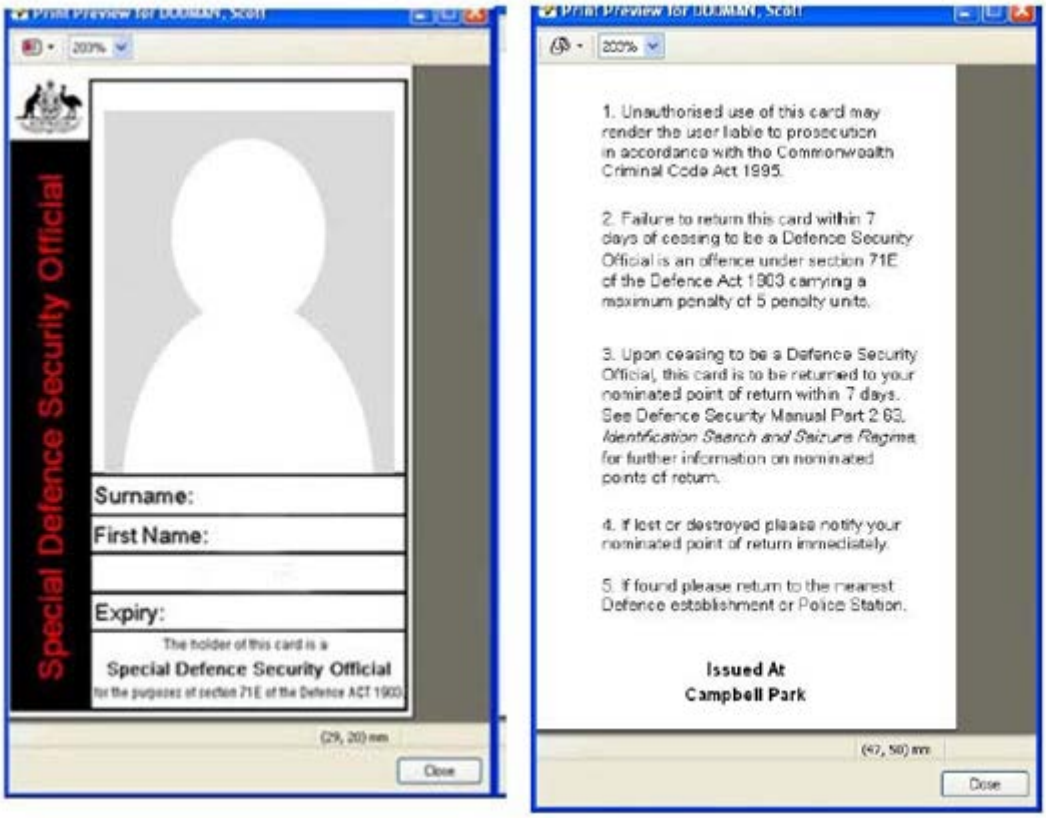
Defence Security Official Identity Card (DSOIC)

Figure 1 – Defence Security Official Identity Card



Special Defence Security Official Identity Card (SDSO)

Figure 2 – Special Defence Security Official Identity Card



Appendixes and Attachments

Appendix 1 – *Defence Security Official Identity Card Delegations*

Document administration

Identification

DSPF Annex	Defence Security Official Identity Cards
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	76.1

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	DG ESD	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Appendix 1 to Annex F of Identification, Search and Seizure Regime – Defence Security Official Identity Card Delegations

Instrument of Delegation

1. A copy of the Secretarial instrument of delegation in relation to the issue and receipt of Defence Security Official Identity Cards is provided below.

Defence Security Official Identity Cards Delegation 2012

Defence Act 1903

I, GREG MORIARTY, Secretary of the Department of Defence, make the following delegation under subsections 71G (1) and (2) of the *Defence Act 1903*.

Dated 6 JULY 2018

SIGNED

Secretary

---

1 Name of delegation

This delegation is the *Defence Security Official Identity Cards Delegation 2012*.

2 Commencement

This delegation commences when it is made.

3 Definitions

In this delegation:

Base Support Manager means a Defence civilian employee or ADF member at the APS Level 5 or equivalent (or military equivalent) or above who is responsible for base support management and services and who has been appointed a Base Support Manager.

Chief Staff Officer Establishments (Navy) means an officer of the Navy who holds the rank of Captain or a higher rank and has been appointed Chief Staff Officer Establishments (Navy).

Deputy Air Commander Australia means an officer of the Air Force who holds the rank of Group Captain or a higher rank and has been appointed Deputy Air Commander Australia.

Director General Capability Planning Air Force means an officer of the Air Force who holds the rank of Group Captain or a higher rank and has been appointed Director General Capability Planning Air Force.

Group Security Adviser means a Defence civilian employee at the Executive Level 2 or above who is the senior security officer in a Group and has been appointed as a Group Security Adviser.

Provost Marshal Australian Defence Force means:

(a) an officer of the Army who holds the rank of Colonel or a higher rank; or

(b) an officer of the Navy who holds the rank of Captain or a higher rank; or

(c) an officer of the Air Force who holds the rank of Group Captain or a higher rank; and

(d) has been appointed Provost Marshall Australian Defence Force.

Regional Director means a Defence civilian employee at the Executive Level 2 or above who has been appointed as a Regional Director within the Defence Support Group.

Security Officer means a Defence civilian employee or ADF member at the APS 5 Level or equivalent (or military equivalent) or above who coordinates or administers the security functions within a business or military unit and has been appointed a Security Officer.

Senior Australian Defence Force Officer (SADFO) means:

(a) an officer of the Army who holds the rank of Colonel or a higher rank; or

(b) an officer of the Navy who holds the rank of Captain or a higher rank; or

(c) an officer of the Air Force who holds the rank of Group Captain or a higher rank; and

(d) has been appointed the SADFO of a base or bases.

Service Security Adviser means:

(a) an officer of the Army who holds the rank of Colonel or a higher rank; or

(b) an officer of the Navy who holds the rank of Captain or a higher rank; or

(c) an officer of the Air Force who holds the rank of Group Captain or a higher rank; and

(d) has been appointed a Service Security Adviser.

4 Delegation

I delegate to each person occupying, or performing the duties of, an office or position mentioned in an item in Schedule 1 my powers or functions under the *Defence Act 1903* mentioned in the item.

Schedule 1Delegation

(section 3)

Item	Provision	Description	Position
1	subsection 71E (1)	To issue an identity card to a defence security official who is a contracted defence security guard	Regional Director, Defence Support Group
2	subsection 71E (1)	To issue an identity card to a defence security official who is: (a) a security authorised member of the Defence Force; and (b) an Identification and Search Warden; and (c) a member of the Service Police	Provost Marshal Australian Defence Force
3	subsection 71E (1)	To issue an identity card to a defence security official who: (a) is a security authorised member of the Defence Force; and (b) is an Identification and Search Warden; and (c) is a member of the Air Force Security Forces	Deputy Air Commander Australia
4	subsection 71E (1)	To issue an identity card to a defence security official who is: (a) a security authorised member of the Defence Force; and (b) is an Identification and Search Warden; and (c) is not a member of the Service Police or a member of the Air Force Security Forces	Senior ADF Officer (***SADFO***) Group Security Adviser Service Security Adviser
5	subsection 71E (1)	To issue an identity card to a defence security official who is: (a) a security authorised member of the Defence Force; and (b) an Armed Security Warden; and (c) performing duties at a base at which enhanced self-defence capability is in operation	Senior ADF Officer (***SADFO***) of a base at which the enhanced self-defence capability is in operation

Item	Provision	Description	Position
6	subsection 71E (1)	To issue an identity card to a defence security official who is: (a) a security authorised member of the Defence Force; and (b) an Armed Security Warden; and (c) performing duties at Fleet Base East	Chief Staff Officer Establishments (Navy)
7	subsection 71E (1)	To issue an identity card to a defence security official who is: (a) a security authorised member of the Defence Force; and (b) a Military Working Dog Handler	Provost Marshal Australian Defence Force Director General Capability Planning Air Force
8	subsection 71E (1)	To issue an identity card to a defence security screening employee	Group Security Adviser Service Security Adviser
9	paragraph 71E (3) (c)	To receive an identity card that is being returned by a defence security official who is a contracted defence security guard	Security Officer Base Support Manager
10	paragraph 71E (3) (c)	To receive an identity card that is being returned by a defence security official who is: (a) a security authorised member of the Defence Force; and (b) an Identification and Search Warden	Security Officer Base Support Manager
11	paragraph 71E (3) (c)	To receive an identity card that is being returned by a defence security official who is: (a) a security authorised member of the Defence Force; and (b) an Armed Security Warden	Security Officer Base Support Manager
12	paragraph 71E (3) (c)	To receive an identity card that is being returned by a defence security official who is: (a) a security authorised member of the Defence Force; and (b) a Military Working Dog Handler	Security Officer Base Support Manager

Attachments

This DSPF Appendix has no Attachments.

Document administration

Identification

DSPF Annex	Defence Security Official Identity Card Delegations
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	76.1

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	DG ESD	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex G to Identification, Search and Seizure Regime – Special Search Provisions for Declared Explosive Ordnance Depots

Special Search Provisions for Declared Explosive Ordnance Depots

1. Given the inherent risk to public safety posed by the unlawful removal of weapons, ammunition and explosive ordnance from Defence premises, special search provisions have been enacted in the *Defence Act 1903* (the Act), Part VIA, Division 3, Subdivision B – Special provisions for declared explosive ordnance depots.

Note: *Not all explosive ordnance depots are covered by the provisions in the Act, Division 3, Subdivision B.*

2. A declared explosive ordnance depot is an area of land, place, building or structure, which is a Defence premise that is used wholly or in part for the storage of explosive ordnance, and where Australian Defence Force members are not normally present. To become a declared explosive ordnance depot, the site must be specified by the Minister in a legislative instrument under the Act, section 71L. In this legislative instrument, the site **must** be referred to either by its:

a. geographical location; or

b. unique code or number.

3. Signs stating that it is a condition of entry to the site that people consent to undergo searches, as provided by the Act Subdivision B, **must** be prominently displayed at the entrance to, and at regular intervals around the perimeter of the declared explosive ordnance depot.

4. Contracted Defence security guards on declared explosive ordnance depots have the same consensual identification and search powers as contracted Defence

security guards at the other Defence premises.[28] Similarly, as at other Defence premises, contracted Defence security guards at declared explosive ordnance depots are not empowered to conduct non-consensual searches.

5. The special provisions for declared explosive ordnance depots empower a contracted Defence security guard to request a consensual limited search of a person or a consensual search of a vehicle anywhere on the depot, not just at an access control point.

6. Under *the Act*, section 71 M a contracted Defence security guard may request a person, who is on a declared explosive ordnance depot, to undergo a consensual limited search of their person, including items in their possession.

7. Under *the Act*, section 71N a contracted Defence security guard may request a person, who is apparently in control of a vehicle on a declared explosive ordnance depot, to permit a consensual search of the vehicle, including things in the vehicle.

8. A contracted Defence security guard may restrain and detain a person, or any other people in the vehicle (for the purpose of handing them over to a state or territory police officer at the earliest practicable time), if:

a. the person refuses the consensual request; or

b. as a result of complying with the request, the contracted Defence security guard reasonably believes that the person or vehicle, including a thing in the vehicle:

(1) is not authorised to be on the declared explosive ordnance depot;

(2) constitutes a threat to the safety of people on the declared explosive ordnance depot;

(3) in the case of a person, has or may commit a criminal offence on, or in relation to the declared explosive ordnance depot; or

(4) in the case of a vehicle, relates to a criminal offence that has or may be committed on, or in relation to the depot.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

---

[28] Refer to DSPF Control 76.1 *Identification, Search and Seizure Regime* paragraphs 20 to 23 and 45 to 53 for further information

Document administration

Identification

DSPF Annex	Special Search Provisions For Declared Explosive Ordnance Depots
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Identification, Search and Seizure Regime
DSPF Number	76.1

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	DG ESD	Launch

Defence Security Principles Framework (DSPF)

Security Incidents and Investigations

General principle

1. Defence will ensure that all security incidents are properly reported and investigated and dealt with in accordance with the relevant policies and legislation.

Rationale

2. Defence's ability to detect, assess and mitigate security vulnerabilities is dependent upon accurate, timely and consistent reporting of all security incidents from across Defence.

3. Information collected through incident reporting and security investigations helps Defence identify security threats, risks and vulnerabilities, evaluate the effectiveness of security controls, develop and improve security policy, make informed and data driven security decisions, and identify security review priorities.

4. Timely and appropriate management of security incidents also helps Defence contain the effects of security incidents, and to recover more rapidly from adverse security events through effective consequence management.

Expected outcomes

5. The security of Defence is enhanced through the reporting and appropriate investigation of security incidents.

6. Defence personnel report security incidents in a timely manner to the relevant authorities.

7. Defence has a comprehensive and accurate database of security incidents to inform risk judgements and assess security trends.

Escalation Thresholds

Risk Rating	Responsibility
Low	Director Security Incident Support and Response (DSIS&R) or Assistant Secretary Security Threat and Assurance (ASSTA) nominated representative.
Moderate	DSIS&R or a Control Owner nominated representative
Significant	DSIS&R or a Control Owner nominated representative
High	ASSTA
Extreme	ASSTA

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Security Incidents and Investigations
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 77
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 77.1
Control Owner	ASSTA

Related information

Government Compliance	**PSPF Core Requirements**: Reporting on Security. Australian Government Protective security governance guidelines – Reporting incidents and conducting security investigations Standards: Australian Government Investigations Standards 2011
Read in conjunction with	N/A
See also DSPF Principle(s)	Contact Reporting
Implementation Notes, Resources and Tools	Interim Defence Instruction Administration 45-2 Incident Reporting and Management Incident Reporting and Management Manual Australian Government Protective security governance guidelines – Reporting incidents and conducting security investigations Australian Government Investigations Standards 2011

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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Security Incidents and Investigations

Control Owner

1. The Assistant Secretary Security Threat and Assurance (ASSTA) is the owner of this Enterprise-wide Control.

Escalation Thresholds

2. The ASSTA 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	Director Security Incident Support and Response (DSIS&R) or ASSTA nominated representative.
Moderate	DSIS&R or a Control Owner nominated representative
Significant	DSIS&R or a Control Owner nominated representative
High	ASSTA
Extreme	ASSTA

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Definition of a Security Incident

3. A security incident is an occurrence which results, or may result, in negative consequences for the security of Defence

4. A *Minor* security incident is an accidental or unintentional action involving failure to observe protective security policy mandatory requirements or procedures within the *Defence Security Principles Framework*. Examples include:

a. access passes or identification documents lost or left insecure; or

b. security classified material not properly secured or stored.

5. A *Major* security incident is any deliberate, negligent or reckless action that leads, or could lead, to the loss, damage, corruption or disclosure of official information or assets. Examples include:

a. the loss of material classified CONFIDENTIAL or above, or significant quantities of material of a lower classification;

b. actual or suspected hacking into any information and communications technology (ICT) system;

c. compromise of security keys or combination locks;

d. actual or attempted unauthorised access to an alarm system covering a secured area where security classified information is stored; or

e. repeated incidents involving the same person or work area where the combination of the incidents warrants an investigation.

6. A *Reportable Major* security incident is any occurrence requiring reporting to the Australian Security Intelligence Organisation (ASIO) as defined I the ASIO Act (1979), including espionage or suspected espionage.

7. An assessment of the harm resulting from a security incident should be used in conjunction with the definitions above to assist in determining whether the incident is a *Minor*, *Major* or *Reportable Major* security incident.

Process

Security Incident Reporting

8. All security incidents must be reported in accordance with the Incident Reporting and Management Manual. The reporting process is as follows:

a. the incident should first be reported to the relevant Commander/Manager/Security Officer;

b. all security incidents are to be reported using the online form *XP188 Security Incident Report*;

c. reports are to be submitted to the Security Incident Centre (SIC) in the following timeframes:

   i. ASIO reportable security incidents immediately (the SIC will advise what further action is required). These security incidents involve activities which fall within the definition of ‘security’ in the *ASIO Act 1979*, and may include:

1. Espionage.

2. Sabotage.

3. Acts of foreign interference.

4. Attacks on Australia's defence system.

5. Politically motivated violence (e.g. terrorism and violent issue-motivated acts).

ii. Major security incidents within 24 hours, noting shorter timeframes for certain incidents listed under 'Special Reporting Requirements'.

iii. Minor security incidents within 30 days.

9. All security incident reports are to contain an assessment of harm resulting from the incident. Management of the incident is to be commensurate with the harm.

10. Security incident reports are only to be classified to the level of sensitivity of the information contained within the report, regardless of the highest classification of the information or asset suspected of compromise. However, the report is to reflect the involvement of the highest classification of information or asset suspected of compromise.

11. Any associated documentation, such as any report resulting from Fact Finding or other administrative inquiry, is to be provided to the SIC. For further information on Fact Finding refer to 'Good Decision-Making in Defence; A guide for Decision-Makers and those who brief them.

12. The Security Officer undertakes the security incident reporting duties on behalf of their Commander or Manager. However, overall management of the incident and reporting process remains the responsibility of the Commander or Manager. While in the first instance security incidents should be reported to the relevant Commander or Manager, and/or the Security Officer, if the Security Officer is unavailable the individual identifying the incident is to report the incident as soon as practicable.

Special Reporting Requirements

13. Commanders and Managers are responsible for managing incidents including chain of command reporting and any special reporting requirements associated with the incident, including but not limited to:

a. ICT security incidents.

b. Asset loss.

c. Radioactive sources.

d. Weapons and explosive ordnance.

e. Free From Explosive violations.

f. Communications security and cryptography.

g. Contacts of security concern.

h. Suspected reconnaissance.

i. Cabinet material.

j. Anonymous reporting and Public Interest Disclosure.

k. Personal Information and Notifiable Data Breaches.

14. Annex A to this DSPF Control provides further information about special reporting requirements.

Security Investigations

15. Where a security incident is sufficiently complex or serious in consequence then responsibility for investigating the incident will be transferred from Commanders and Managers to a Defence Investigative Authority (DIA) in accordance with Australian Government Protective security governance guidelines – Reporting incidents and conducting security investigations. The SIC will determine which security incidents will be subject to further formal investigation in consultation with the relevant DIA. Commanders and Managers are to continue managing the incident in consultation with the DIA.

16. Notwithstanding the legal rights of a person under investigation, Defence personnel, Contractors, Consultants and Outsourced Service Providers are to:

a. comply with lawful directions during the conduct of an investigation;

b. not hinder a security investigations; and

c. not reveal any aspect of an investigation to anyone without the prior approval of the investigator.

Outcome of Investigations

17. At the completion of an investigation into a security incident the DIA will provide an investigation report detailing the findings and recommendations of the investigation.

18. The DIA will ensure that recommendations from the investigation are assigned for implementation to all areas of Defence and Defence industry affected by the recommendations.

19. An SES Band 1/ADF O7 level officer will be responsible for implementing the investigation's recommendations.

Roles and Responsibilities

Assistant Secretary Security Threat and Assurance (ASSTA)

20. The ASSTA is responsible for:

a. ensuring that reported security incidents have been logged onto the Defence Policing and Security Management System (DPSMS). DS&VS may refer incidents back to the reporting unit to be managed at the local level;

b. analysing reported security incidents;

c. determining which incidents require investigations;

d. reporting data spills or incidents that involve unauthorised access to classified information via an ICT system to the Defence Information Technology Security Adviser;

e. determining the most appropriate DIA, civil authority or unit to conduct an investigation or administrative inquiry in the event of a major security incident;

f. consulting with ASIO and other law enforcement agencies prior to commencing an investigation to determine which agency will take responsibility for investigating an ASIO reportable security incident; and

g. the provision of advice regarding security incident reporting and security investigations.

Chief Information Officer (CIO)

21. The Chief Information Officer (CIO) is the capability manager for the Single Information Environment (SIE) and is responsible for setting the strategic direction of the SIE which will include the management of information systems security incidents. Key responsibilities include:

a. Protecting the SIE and preventing ICT security incidents at Defence network gateways. This includes the blocking of files and emails that pose a security or denial of service threat;

b. Ensuring that any suspected or successful ICT attacks or other major ICT security incidents are reported to the SIC and the ASD. ICT attacks include:

   i. unauthorised intrusion into a Defence ICT system (hacking);

   ii. the compromise or corruption of official or classified information on a Defence ICT system;

   iii. the introduction of viruses to a Defence ICT system;

   iv. the intentional or accidental disruption to an ICT service; and

   v. the loss or theft of Defence ICT equipment.

Note: *The ICT security incidents listed above are to be recorded in DPSMS and reported to the SIC, which will determine which incidents will be subject to investigation by the DS&VS or will determine the appropriate DIA for such investigation.*

c. Managing unsuccessful ICT attacks (including unsuccessful attempts to hack, compromise, corrupt or disrupt Defence ICT systems or services, introduce a virus to a Defence ICT system, or steal Defence ICT equipment) locally;

d. Managing communications security (COMSEC) incidents, through the Defence Cryptographic Controlling Authority, in accordance with the procedures contained in Australian Communications Security Instruction (ACSI) 107B Reporting and Evaluating COMSEC Incidents and Australian Defence Force Publication (ADFP) 6.0.3.1 Communications Security Instructions; and

e. Providing a monthly report to the FAS S&VS detailing the number and types of incidents detected as well as the number of open incidents that are yet to be categorised, referred or investigated.

Security Incident Centre (SIC)

22. The SIC, in DS&VS, is the Defence element responsible for the assessment, referral and monitoring as required, of security incidents in Defence and Defence industry.

Defence Investigative Authorities (DIAs)

23. A DIA is a Defence body given the authority by the Secretary and the Chief of Defence Force to undertake investigations. DIA are authorised and required to conduct independent investigations (where they have jurisdiction), unfettered by the chain of command or line management, into suspected major security incidents.

24. It is the responsibility of the DIA to:

a. conduct investigations in accordance with:

   i. the Australian Government Protective security governance guidelines – Reporting incidents and conducting security investigations;

   ii. Interim Defence Instruction Administration 45-2 Incident Reporting and Management;

   iii. The Australian Government Investigation Standards; and

   iv. this policy.

b. log security investigations reported to the DIA onto the Defence Policing and Security Management System; and

c. inform the Australian Government Security Vetting Agency where an investigation makes an adverse finding against an individual, including where the event was accidental.

Commanders and Managers

25. Commanders and Managers are responsible for ensuring that:

a. security incidents are appropriately managed to completion;

b. they and their staff are aware of, and comply with, the requirement to report and manage all security incidents; and

c. ensure that all security incidents that occur within their military or business unit are recorded in the security register.

Annexes and Attachments

Annex A – *Special Reporting Requirements*

Document administration

Identification

DSPF Control	Security Incidents and Investigations
Control Owner	Assistant Secretary Security Threat and Assurance
DSPF Number	Control 77.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Security Incidents and Investigations
Related DSPF Control(s)	N/A

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	ASSTA	Launch

Defence Security Principles Framework (DSPF)

Annex A to Security Incidents and Investigations – Special Reporting Requirements

ICT Security Incidents

1. In the case of major ICT security incidents involving data spills, virus or malicious software attacks, the responsible Commander or Manager is to:

a. report the incident to the Defence Information Technology Security Advisor (ITSA); and

b. under the direction of the Defence ITSA, minimise the impact to Defence ICT systems.

Asset Loss

2. In the case of a loss of asset in any manner (deliberate or accidental), the loss may have to be reported as a financial incident in addition to a security incident. For further information, refer to the Financial Management Manual 5 (FINMAN 5).

3. Loss of controlled items, including Defence and dual-use goods, technology acquired under licence and technology subject to export controls, may have additional reporting requirements. The Defence Export Control Branch and the Defence Logistics Manual (DEFLOGMAN) should be consulted in these cases.

Radioactive Sources

4. Where a security incident involves a sealed radioactive source, the Australian Government Code of Practice for the Security of Radioactive Sources takes precedence over the DSPF and specific incident notification requirements apply for immediate notification to appropriate authorities. For further information see DSPF Principle 80 – *Security of Radioactive Sources*.

Weapons and Explosive Ordnance

5. On discovering the loss or suspected loss, theft or attempted theft, recovery, discovery or suspicious incidents involving Defence weapons, cadet firearms, associated equipment related to weapons, or explosive ordnance the person in charge is required to:

a. immediately report the matter to the appropriate authority in their Group or Service;

b. notify the local civilian police;

c. notify the Stock Item Owner within 24 hours; and

d. report the incident to the Security Incident Centre (SIC) immediately.

6. An information copy of the report to the Group Head or Service Chief is to also be supplied to the First Assistant Secretary Security and Vetting Service (FAS S&VS).

Free From Explosive violations

7. Free From Explosive (FFE) violations involving Small Arms Ammunition (SAA) are not considered a major security incident and are to be reported to the Explosive Ordnance Incident Administration Cell (EOIAC) in accordance with eDEOP 101 – Regulation 1.3 using Web Form EO 016 Explosive Ordnance Security Incident Report. To meet the intent of this exclusion, the live explosive ordnance discovered in certified FFE returns are found in an approved Explosive Ordnance (EO) container and/or packaging that has been appropriately affixed with a certified (signed IAW eDEOP 101 – Regulation 2.3 Procedure 5) Form EO 052 ‘Certified Empty (FFE)’ label or approved equivalent.

8. FFE violations reported to the EOIAC where ‘bulk’ or ‘large’ quantities of live SAA are found in approved EO containers or packaging certified FFE will be escalated to the SIC as a major security incident by the EOIAC via an XP188 form.

9. FFE violations involving explosive ordnance other than SAA are considered a major security incident. They are to be handled in accordance with Interim Defence Instruction Administration 45-2 Incident Reporting and Management and are to be reported to:

a. the SIC using an XP188 form; and

b. the EOIAC and Joint Logistics Unit Regional Explosive Ordnance Section via Web Form EO 016 Explosive Ordnance Security Incident Report in accordance with eDEOP 101 Regulation.

Communications security and cryptography

10. Communications security and cryptography breaches, including the loss or recovery of any cryptographic controlled item where there is no suspicion of espionage, are to be reported directly to the Defence Cryptographic Controlling Authority in accordance with the reporting procedures contained in Australian Communications Security Instruction (ACSI) 107B Reporting and Evaluating COMSEC Incidents and Australian Defence Force Publication (ADFP) 6.0.3.1 Communications Security Instructions, and to the SIC.

Contacts of security concern

11. Suspicious contact of security concern is any contact which could be regarded as suspicious, persistent or out of the ordinary. All contacts of security concern are to be reported on the relevant form in accordance with the DSPF Principle 45 - *Contact Reporting*.

Suspected reconnaissance

12. Suspicious behaviour including persons engaged in reconnaissance, surveillance, photography or trespass of or on Defence or Defence industry sites are to be reported on an XP188 Security Incident Report form and forwarded to the SIC within 24 hours.

Reporting the loss of classified information

13. Depending on the classification of information, loss is either a minor or major security incident. The loss is to be reported in accordance with normal procedure. However, if the reporting entity/unit is not the information originator, then the originator, if identified and located, is to be notified and asked to provide a damage assessment. If the originator cannot be identified or located, it is recommended that a subject matter expert is identified and consulted to assist with the damage assessment.

14. The reporting area for the loss is to provide the following information to an SES Band 1/ADF O7 level officer within the reporting area's line management or chain of command before write-off action can be authorised by that SES Band 1/ADF O7 level officer:

a. the information to be written off;

b. the classification level(s) of the information;

c. the damage assessment (whether on the original XP188 or subsequently provided); and

d. a copy of any associated documentation:

(1) a Minute requesting write-off approval from the relevant SES Band 1 / ADF 07, to be signed by the Commander or Manger;

(2) any FACT Finding or administrative inquiry report;

(3) any investigation report provided by a Defence Invetigative Authority.

15. Following approval to write off classified information:

a. the lost information entries are to be identified in the Classified Document Register (CDR);

b. the serial number in the CDR is to be ruled out and all relevant information annotated in the 'remarks' column;

c. any records relating to the lost information is to be correctly amended and, where lost information is replaced, the new entry needs to be cross-referenced to the original entry;

d. an independent officer is to record their signature to each serial that is declared missing in the CDR;

e. any other record(s) listing the lost information is to be amended accordingly; and

f. a copy of the approved minute requesting write-off together with any Annexes and Enclosures is to be sent via email to the SIC.

Cabinet Material

16. Relevant Commanders or Managers are to report suspected security incidents involving Cabinet material to the Cabinet Secretariat in the Department of the Prime Minister and Cabinet. The Cabinet Handbook provides information about the security and handling of Cabinet documents.

Anonymous Reporting and Public Interest Disclosure

17. Defence encourages employees and external service providers who have serious security concerns and believe themselves to be at risk of recriminations if they report a security incident to use the reporting provisions of the Defence Public Interest Disclosure scheme.

Personal Information and Notifiable Data Breaches

18. Incidents involving the disclosure of personal information need to consider management and reporting requirements of the Notifiable Data Breach scheme (established under Part IIIC of the *Privacy ACT 1988 (Cth)*).

19. Under the Notifiable Data Breach scheme, Defence is required to notify individuals whose personal information is involved in a data breach that is likely to result in serious harm. Such breaches are referred to as 'eligible data breaches'. Notifications must include recommendations regarding the steps individuals should take in response to the breach.

20. Further information in relation to the Notifiable Data Breach scheme, including management and response to data breaches, is available on the Office of the Australian Information Commissioner website (https://www.oaic.gov.au/privacy-law/privacy-act/notifiable-data-breaches-scheme).

21. Data breaches, including suspected eligible data breaches, are to be managed by the area collecting the personal information and responsible for its protection and security.

22. Suspected eligible data breaches are to be notified to Defence Privacy who will advise commanders and managers regarding reporting to the Office of the Australian Information Commissioner.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Special Reporting Requirements
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Security Incidents and Investigations
DSPF Number	Control 77.1

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	ASSTA	Launch

Defence Security Principles Framework (DSPF)

Weapons Security

General principle

1. All Defence weapons and Cadet Firearms are to be secured or controlled to prevent loss, theft or misuse. Defence weapons are to be stored in accordance with Defence security policy.

Rationale

2. Defence holds weapons that are illegal for possession by the general population. This makes Defence weapons attractive to criminal elements, including extremist organisations and malicious trusted insiders. As a result, there is an increased risk that criminal elements may target Defence armouries, repair facilities, personnel, and associated transportation activities as potential sources of these items.

3. There is also a significant potential risk to weapons security from Defence personnel and external service providers. Theft by Defence personnel or external service providers can be opportunistic and can occur where supervision and checking procedures have not properly taken account of this threat.

Expected outcomes

4. Defence weapons are adequately stored to prevent loss, theft and misuse.

5. Only appropriately cleared and trained personnel have access to Defence weapons.

6. Defence has controls or procedures in place to detect the loss, theft and attempted theft of weapons within specific timeframes.

Escalation Thresholds

Risk Rating	Responsibility
Low	O4 or APS 6 or equivalent in the relevant Group/Service
Moderate	O5 or EL 1 or equivalent in relevant Group/Service
Significant	Assistant Secretary Security Policy and Services (AS SPS)
High	Defence Security Committee (DSC) – through AS SPS
Extreme	Defence Security Committee (DSC) – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Note: *Chief of Joint Operations (CJOPS) or an authorised delegate can accept significant to extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.*

Document administration

Identification

DSPF Principle	Weapons Security
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 78
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 78.1
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)

Related information

Government Compliance	**PSPF Core Requirements:** Security planning; Security governance for international sharing; and Entity physical resources. **Legislation:** *Workplace Health and Safety Act 2011* (Cth)
Read in conjunction with	Interim Capability Life Cycle Manual Estimates Memorandum 2015/51 – Defence Specific Costing Requirements for Projects in the Defence Integrated Investment Programme.
See also DSPF Principle(s)	Security Incidents and Investigations Physical Transfer of Official Information, Security Protected and Classified Assets Physical Security Escorting Security Protected or Classified Assets SAFEBASE
Implementation Notes, Resources and Tools	Australian Government physical security management protocol: https://www.protectivesecurity.gov.au/physicalsecurity/Pages/Protocol.aspx Security Equipment Guides (SEGs) via the Security Toolkit. ASIO Tech Notes via the Security Toolkit. Security Equipment Evaluated Product List (SEEPL). This list contains products endorsed by the Security Construction and Equipment Committee (SCEC). Contact the Protective Security Advice Centre PSAC, your Executive Security Advisor (ESA), or your DS&VS regional office for further information.

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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Weapons Security

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The First Assistant Secretary, Security and Vetting Service (FAS S&VS), is the owner of this enterprise wide control.

Control

2. This section of this DSPF Enterprise-wide Control is For Official Use Only and has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – *Storage Requirements for Weapons*

Annex B – *Storage and Management of Privately Owned Weapons and Ammunition*

Annex C – *Armouries*

Annex D – *Transporting Defence Weapons*

Annex E – *Security Requirements for Display and Demonstration of Weapons*

Document Administration

Identification

DSPF control	Weapons Security
Control Owner	First Assistant Secretary, Security and Vetting Service
DSPF number	Control 78.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Principle 78 Weapons Security
Related DSPF Control(s)	Physical Transfer of Information and Assets Physical Security Security Incidents and Investigations Escorting Security Protected of Classified Assets SAFEBASE

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 SPS	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex A – Storage Requirements for Weapons

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The First Assistant Secretary, Security and Vetting Service (FAS S&VS) is the owner of this enterprise-wide annex.

Control

2. This section of this DSPF Enterprise-wide Annex is For Official Use Only and has been removed from this version. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Appendixes and Attachments

Appendix 1 – *Ceasing Periodic Checks during an Extended Reduced Activity Period*

Document administration

Identification

DSPF Annex	Storage Requirements for Weapons
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

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 SPS	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Appendix 1 to Annex A – Ceasing Periodic Checks During an Extended Reduced Activity Period

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Appendix. To view the full Appendix, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The First Assistant Secretary, Security and Vetting Service (FAS S&VS) is the owner of this enterprise-wide appendix.

Control

2. This section of this DSPF Enterprise-wide Appendix is For Official Use Only and has been removed from this version. To view the full Appendix, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Ceasing Periodic Checks During an Extended Reduced Activity Period
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security

DSPF Annex	Ceasing Periodic Checks During an Extended Reduced Activity Period
DSPF Number	Control 78.1

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 SPS	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B – Storage and Management of Privately Owned Weapons and Ammunition

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The First Assistant Secretary, Security and Vetting Service (FAS S&VS) is the owner of this enterprise-wide annex.

Control

2. This section of this DSPF Enterprise-wide Annex is For Official Use Only and has been removed from this version. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Storage and Management of Privately Owned Weapons and Ammunition
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

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 SPS	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex C – Armouries

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The First Assistant Secretary, Security and Vetting Service (FAS S&VS) is the owner of this enterprise-wide annex.

Control

2. This section of this DSPF Enterprise-wide Annex is For Official Use Only and has been removed from this version. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no appendixes or attachments.

Document administration

Identification

DSPF Annex	Armouries
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

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 SPS	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex D – Transporting Defence Weapons

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The First Assistant Secretary, Security and Vetting Service (FAS S&VS) is the owner of this enterprise-wide annex.

Control

2. This section of this DSPF Enterprise-wide Annex is For Official Use Only and has been removed from this version. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Transporting Defence Weapons
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	Control 78.1

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 SPS	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex E – Security Requirements for Display and Demonstration of Weapons

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The First Assistant Secretary, Security and Vetting Service (FAS S&VS) is the owner of this enterprise-wide annex.

Control

2. This section of this DSPF Enterprise-wide Annex is For Official Use Only and has been removed from this version. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Appendixes and Attachments

Appendix 1 – *Mounting Procedures for Small and Trophy Weapons*

Document Administration

Identification

DSPF Annex	Weapons Security
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	78.1

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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Appendix 1 to Annex E – Mounting Procedures for Small and Trophy Weapons

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Appendix. To view the full Appendix, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The First Assistant Secretary, Security and Vetting Service (FAS S&VS) is the owner of this enterprise-wide appendix.

Control

2. This section of this DSPF Enterprise-wide Appendix is For Official Use Only and has been removed from this version. To view the full Appendix, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Attachments

This Appendix currently has no Attachments.

Document administration

Identification

DSPF Annex	Mounting Procedures for Small and Trophy Weapons
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Weapons Security
DSPF Number	78.1

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

Defence Security Principles Framework (DSPF)

Explosive Ordnance Security

General principle

1. Explosive Ordnance (EO) must be secured from theft, loss and misdirection in compliance with relevant legislation, Defence regulations and Australian Government codes. Additional controls should reduce the risk of theft, loss and misdirection of these assets to a level that is as low as reasonably practicable. Live EO held by Defence will be managed as security protected assets or is applicable, as classified assets.

Rationale

2. Military EO is highly prized by extremist and criminal organisations. This, coupled with the unavailability of many Defence EO items commercially, increases the risk that extremist or criminal elements may target Defence EO storage facilities and associated transportation activities as potential sources of these items.

3. There is also a significant potential risk to EO security from Defence personnel, Contractors, Consultants and Outsourced Service Providers. Theft by these persons can be opportunistic and occur where supervision and checking procedures have not properly taken account of this threat.

Expected outcomes

4. Defence personnel, Contractors, Consultants and Outsourced Service Providers are responsible for securing and controlling EO. They are also responsible to prevent its loss, theft or misdirection. EO is to be secured during storage and transport in accordance with Defence security controls, process and instructions. Access to EO is to be strictly controlled. EO may only be issued to individuals who are authorised to receive it and who accept responsibility for the safekeeping of that EO.

5. Where there is a conflict between safety and security requirements, the issue is to be referred to the Explosive Ordnance Branch, Joint Logistics Command for determination of the requirement.

Escalation Thresholds

Risk Rating	Responsibility
Low	O4 or APS6 or equivalent in relevant Group/Service
Moderate	O5 or EL1 or equivalent in relevant Group/Service
Significant	Director General (DG) or O6 or EL2 or equivalent in relevant Group/Service
High	Defence Security Committee (DSC) via Commander Joint Logistics (CJLOG)
Extreme	DSC via CJLOG

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Note: *Chief of Joint Operations (CJOPS) or an authorised delegate can accept significant to extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.*

Document administration

Identification

DSPF Principle	Explosive Ordnance Security
Principle Owner	First Assistant Secretary Security & Vetting Service (FAS S&VS)
DSPF Number	Principle 79
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 79.1
Control Owner	Commander Joint Logistics Group

Related information

Government Compliance	**PSPF Core Requirements**: Security planning; Security governance for international sharing; Entity physical resources; and Entity facilities. **Legislation**: Explosives Transport Regulations 2002 (Cth) Australian Code for the Transport of Explosives by Road and Rail (AEC 3)
Read in conjunction with	N/A
See also DSPF Principle(s)	Personnel Security Clearance Temporary Access to Classified Information and Assets Physical Security Physical Security Certification and Accreditation Access Control Contracted Security Guards Security Incidents and Investigations Escorting Security Protected or Classified Assets
Implementation Notes, Resources and Tools	DI(G) LOG 4-1-006: Safety of Explosive Ordnance DI(G) LOG 4-5-012: Regulation of technical integrity of Australian Defence Force materiel Australian Code for the Transport of Explosives by Road and Rail (AEC) eDEOP 100 - Defence Explosive Ordnance Publication eDEOP 101 - Department of Defence Explosives Regulations

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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Explosive Ordnance Security

Redacted Versione: *Official content has been removed from this DSPF Enterprise-wide Control. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The Commander Joint Logistics Group (CJLOG) is the owner of this Enterprise-wide Control.

Control

2. This section of this DSPF Enterprise-wide Control is For Official Use Only and has been removed from this version. To view the full Control, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Further Definitions

3. Further definitions for common PSPF terms can be found in the Glossary.

4. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes

Annex A – *Storage of Explosive Ordnance*

Annex B – *Transport Procedures for Explosive Ordnance*

Annex C – *Security Requirements for Control of Inert Explosive Ordnance*

Annex D – *Storage and Management of Privately Owned Explosive Ordnance*

Document administration

Identification

DSPF Control	Explosive Ordnance Security
Control Owner	Commander Joint Logistics Group (CJLOG)
DSPF number	Control 79.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Explosive Ordnance Security
Related DSPF Control(s)	Personnel Security Clearance Temporary Access to Classified Information and Assets Physical Security Physical Security Certification and Accreditation Access Control Contracted Security Guards Security Incidents and Investigations Escorting Security Protected or Classified Assets

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	CJLOG	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex A to Explosive Ordnance Security – Storage of Explosive Ordnance

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The Commander Joint Logistics Group (CJLOG) is the owner of this enterprise-wide annex.

Control

2. This section of this DSPF Enterprise-wide Annex is For Official Use Only and has been removed from this version. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Appendix

Appendix 1 – *Ceasing Periodic Checks During an Extended Reduced Activity Period*.

Document administration

Identification

DSPF Annex	Storage of Explosive Ordnance
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Explosive Ordnance Security
DSPF Number	Control 79.1

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	CJLOG	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Appendix 1 to Annex A of Explosive Ordnance Security – Ceasing Periodic Checks during an Extended Reduced Activity Period

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Appendix. To view the full Appendix, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The Commander Joint Logistics Group (CJLOG) is the owner of this enterprise-wide appendix.

Control

2. This section of this DSPF Enterprise-wide Appendix is For Official Use Only and has been removed from this version. To view the full Appendix, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Ceasing Periodic Checks during an Extended Reduced Activity Period
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Explosive Ordnance Security
DSPF Number	Control 79.1

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	CJLOG	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B to Explosive Ordnance Security – Transport Procedures for Explosive Ordnance

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The Commander Joint Logistics Group (CJLOG) is the owner of this enterprise-wide annex.

Control

2. This section of this DSPF Enterprise-wide Annex is For Official Use Only and has been removed from this version. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendices or Attachments.

Document administration

Identification

DSPF Annex	Transport Procedures for Explosive Ordnance
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Explosive Ordnance Security
DSPF Number	Control 79.1

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	CJLOG	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex C to Explosive Ordnance Security – Security Requirements for Control of Inert Explosive Ordnance

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The Commander Joint Logistics Group (CJLOG) is the owner of this enterprise-wide annex.

Control

2. This section of this DSPF Enterprise-wide Annex is For Official Use Only and has been removed from this version. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Appendixes and Attachments

Appendix 1 – *Security Requirements for Display and Demonstration of Inert Explosive Ordnance*

Document administration

Identification

DSPF Annex	Security Requirements for Control of Inert Explosive Ordnance
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Explosive Ordnance Security
DSPF Number	Control 79.1

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	CJLOG	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Appendix 1 to Annex C of Explosive Ordnance Security – Security Requirements for Display and Demonstration of Inert Explosive Ordnance

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Appendix. To view the full Appendix, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The Commander Joint Logistics Group (CJLOG) is the owner of this enterprise-wide appendix.

Control

2. This section of this DSPF Enterprise-wide Appendix is For Official Use Only and has been removed from this version. To view the full Appendix, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Attachments

This DSPF Appendix has no Attachments.

Document administration

Identification

DSPF Annex	Security Requirements for Display and Demonstration of Inert Explosive Ordnance
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Explosive Ordnance Security
DSPF Number	Control 79.1

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	CJLOG	Launch

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex D to Explosive Ordnance Security – Storage and Management of Privately Owned Explosive Ordnance

Redacted Version: *Official content has been removed from this DSPF Enterprise-wide Annex. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.*

Control Owner

1. The Commander Joint Logistics Group (CJLOG) is the owner of this enterprise-wide annex.

Control

2. This section of this DSPF Enterprise-wide Annex is For Official Use Only and has been removed from this version. To view the full Annex, visit the DSPF Defence Restricted Network (DRN) site or contact your contract manager.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document administration

Identification

DSPF Annex	Storage and Management of Privately Owned Explosive Ordnance
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Explosive Ordnance Security
DSPF Number	Control 79.1

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	CJLOG	Launch

Defence Security Principles Framework (DSPF)

Radioactive Sources

General principle

1. Security Enhanced Sources must be secured from theft, loss or unauthorised access in full compliance with the Commonwealth Code of Practice for the Security of Radioactive Sources (RPS 11).

Rationale

2. Defence deals with its radioactive sources in accordance with the conditions attached to the Defence Source Licence, which is issued by the Australian Radiation Protection and Nuclear Safety Agency (ARPANSA). The normal security protocols within Defence, which are in place for safety purposes, are considered to be adequate to ensure the physical security of the majority of radioactive sources.

3. A sealed radioactive source consists of radioactive material that is either permanently contained in a capsule or is closely bound in solid form. They are categorised on the basis of their risk, from Category 1 (high) to Category 5 (low). The loss or compromise of any sealed radioactive source will have safety and security ramifications that could negatively impact on Defence's personnel and its reputation.

4. A Security Enhanced Source is defined as a source from Category 1, 2 or 3. Such sources are dangerous to human life in exposure events of a few minutes (Category 1) to a few hours (Category 2) to a few days (Category 3). As such, these sources pose a significant risk to national security if acquired by persons of malicious intent.

Expected outcomes

5. Security Enhanced Sources will be protected against theft, loss or unauthorised access to the full extent of our obligations and in accordance with National and International requirements.

6. Security Enhanced Sources held by Defence will be managed in accordance with the Defence Radiation Safety Manual, Chapter 3, Annex C.

7. Security Enhanced Sources for which Defence is responsible will be secured in full compliance with the Code of Practice for the Security of Radioactive Sources - ARPANSA Radiation Protection Series No.11.

8. Where there is a conflict between safety and security requirements, the issue is to be referred to Director, Defence Radiation Safety and Environment, Joint Logistics Command for determination of the requirement.

Escalation Thresholds

Risk Rating	Responsibility
Low	O4 or APS6 or equivalent in relevant Group/Service
Moderate	O5 or EL1 or equivalent in relevant Group/Service
Significant	Director General (DG) or O6 or EL2 or equivalent in relevant Group/Service
High	Defence Security Committee (DSC) via Commander Joint Logistics (CJLOG)
Extreme	DSC via CJLOG

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Radioactive Sources
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 80
Version	2
Publication date	21 May 2019
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	None
Control Owner	Commander Joint Logistics (CJLOG)

Related information

Government Compliance	**PSPF Core Requirements**: Security planning; Security governance for international sharing; Entity physical resources; and Entity facilities. **Legislation**: *Australian Radiation Protection and Nuclear Safety Act 1998* (the ARPANS Act) *Australian Radiation Protection and Nuclear Safety Regulations 1999* (the ARPANS Regulations) Code of Practice for the Security of Radioactive Sources - ARPANSA Radiation Protection Series No.11 (RPS 11)
Read in conjunction with	Defence Radiation Safety Manual (the DRSM)
See also DSPF Principle(s)	Personnel Security Clearance Physical Security Certification and Accreditation Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	Australian Radiation Protection and Nuclear Safety Act 1998 (the ARPANS Act) Australian Radiation Protection and Nuclear Safety Regulations 1999 (the ARPANS Regulations) Code of Practice for the Security of Radioactive Sources - ARPANSA Radiation Protection Series No.11 (RPS 11) Defence Radiation Safety Manual (the DRSM)

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	21 May 2019	FAS S&VS	Additional clarification added to Rationale

Defence Security Principles Framework (DSPF)

Escorting Security Protected or Classified Assets

General principle

1. Where security considerations demand, specific security-protected assets are to be escorted by appropriately qualified and authorised escorts.

Rationale

2. Loss or theft of security-protected or classified assets impacts Defence capability and reputation.

3. Security-protected or classified assets (such as Weapons and Explosive Ordnance) are highly sought after by criminal and extremist organisations and are vulnerable to theft during transport.

Expected outcomes

4. Security Risk Assessments are used to determine the escort requirements for the transportation of security-protected or classified assets in accordance with the Principle's subordinate Control policy.

5. Escorts are appropriately qualified to secure consignments against theft, loss or misuse during transport;

6. Escorts are aware of their roles and responsibilities; and

7. Any security incidents associated with the transport of security-protected or classified assets are reported appropriately.

Escalation Thresholds

The Assistant Secretary, Security Policy and Services (AS SPS) has set the following general thresholds for risks managed against this *DSPF Enterprise-wide Control* and the related *DSPF Principle and Expected Outcome*.

Weapons and Explosive Ordnance Escorting Risks

Risk Rating	Responsibility
Low	EL2/O-6 or equivalent in relevant Group/Service
Moderate	SES1/O-7 or equivalent in relevant Group/Service
Significant	Defence Security Committee (DSC) – through AS SPS
High	DSC – through AS SPS
Extreme	Defence Security Committee (DSC) – through AS SPS

All Other Security Protected and Classified Assets Escorting Risks

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 SPS
High	DSC – through AS SPS
Extreme	DSC – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Note: *Chief of Joint Operations or an authorised delegate can accept significant to extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.*

Document administration

Identification

DSPF Principle	Escorting Security Protected or Classified Assets
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 81
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	81.1 Escorting Security Protected or Classified Assets
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)

Related information

Government Compliance	**PSPF Core Requirements**: Security governance for contracted service providers; Security governance for international sharing; Eligibility and suitability of personnel; Entity physical security; and Entity facilities. **Legislation**: For all relevant state and territory private security guard legislation, see DSPF Principle 75 - *Contracted Security Guards*. *Explosive Transport Regulations 2002 (Cth)* *Australian Code for the Transport of Explosives by Road and Rail* (AEC 3)
Read in conjunction with	N/A
See also DSPF Principle(s)	Physical Transfer of Information and Assets Physical Security Contracted Security Guards Security Incidents and Investigations Weapons Security Explosive Ordnance Security Security of Radioactive Sources
Implementation Notes, Resources and Tools	DI(G) LOG 4-1-006: Safety of Explosive Ordnance DI(G) LOG 4-5-012: Regulation of technical integrity of Australian Defence Force materiel Australian Code for the Transport of Explosives by Road and Rail (AEC) eDEOP 100 - Defence Explosive Ordnance Publication eDEOP 101 - Department of Defence Explosives Regulations

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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Escorting Security Protected or Classified Assets

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) is the owner of this enterprise-wide control

Escalation Thresholds

2. The AS SPS has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcome

Weapons and Explosive Ordnance Risks

Risk Rating	Responsibility
Low	EL2/O-6 or equivalent in relevant Group/Service
Moderate	SES1/O-7 or equivalent in relevant Group/Service
Significant	Defence Security Committee (DSC) – through AS SPS
High	DSC – through AS SPS
Extreme	DSC – through AS SPS

All Other Security Protected and Classified Assets Escorting Risks

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 SPS
High	DSC – through AS SPS
Extreme	DSC – through AS SPS

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Note: *Chief of Joint Operations (CJOPS) or an authorised delegate can accept significant to extreme risks in areas of operations. The Control Owner is to be advised as soon as is feasible.*

Control

3. This DSPF part provides the base requirements for escorting. Additional controls may apply for the transport of weapons, Explosive Ordnance (EO) and assets with high Business Impact Levels (BILs). For further information, refer to:

a. DSPF Principle 78 - *Weapons Security*;

b. DSPF Principle 79 - *Explosive Ordnance Security*; and

c. DSPF Principle 71 - *Physical Transfer of Information and Assets*.

4. A Movement Security Plan (MSP) should be developed before undertaking escorting activities. A Security Risk Assessment (SRA) should be conducted as part of this process. For further information on Transportation and MSP requirements, see Annex D and Annex E to DSPF Control 71.1 – *Physical Transfer of Information and Assets*.

5. With the exception of mandatory provisions (bold must statements), an SRA can also be used to determine whether a departure from the requirements found throughout this DSPF part is permissible. This risk assessment **must** take the following into consideration:

a. The distance required to transport the security protected asset;

b. The quantity of security protected assets (including EO) being transported; and

c. Relevant threat assessments. Threat assessments can be found on the Defence Secret Network

Note: *in some circumstances, activity specific threat assessments can be requested. See DS&VS Security Threat Assessments.*

6. For further guidance on SRAs, see DS&VS Security Risk Management.

When to Escort

7. There **must** be an escort for the vehicle transport of any quantity of:

a. Weapons;

b. EO; or

c. security-protected assets assigned a BIL of 4 (Extreme) or above (or classified SECRET and above).

8. A risk assessment can be conducted to determine if escorts are required for the transport of security-protected assets assigned a BIL of 3 (Very High) and below (classification of CONFIDENTIAL and below).

9. Escorts are not required:

a. For direct hand carriage of classified information (e.g. between two office buildings), in accordance with DSPF Principle 71 - *Physical Transfer of Information and Assets*;

b. EO recovery activities by EO disposal personnel; and

c. During the sea or air legs of commercial international or domestic transfer

Case Study: *The above requirement does apply, however, for any road or rail transport of security-protected assets before and after any sea/air movement.*

Who Can Escort

10. An escort should have:

a. an understanding of the escorting responsibilities as specified in this DSPF part and their specific escorting instructions;

b. any qualifications and training required to carry out their escorting duties (e.g. weapons training for armed escorts); and

c. as a minimum, the same driver qualifications as the driver of the cargo or escort vehicle in order to drive the vehicle in an emergency.

11. When considering fatigue management, escorts and drivers may switch roles if the driver has the requisite qualifications and training to act as an escort; however, for long hauls, it is recommended that additional drivers are available.

Note: *escorts should be made aware of their responsibilities and the extent of their powers to prevent unauthorised access to the consignment.*

Note: *Estate and Infrastructure Group often manage offsite classified waste disposal for Defence sites. APS members are regularly employed to act as escorts during these activities. In accordance with their MSP, the escorts are required to follow the waste vehicles and witness the disposals. They are instructed to alert the local police of unauthorised attempts to access the waste and report incidents in accordance with DSPF Principle 77 - Security Incidents and Investigations.*

Officer in Charge

12. Where there is more than one escort, the most senior escort is designated Officer in Charge (OIC) of the escort party and should travel in the escort vehicle. For Defence personnel, the OIC should be at least a Junior Non-Commissioned Officer (NCO) (Leading Seaman, Corporal, or Lance Corporal) or an Australian Public Service (APS) equivalent. For large or sensitive consignments it is recommended that the OIC be at least a Senior NCO or APS equivalent. If Australian Federal Police (AFP), AFP Protective Services (AFP-PS) or state and territory police are providing escorts, they will allocate an OIC at a level they deem appropriate.

Armed Escorts

13. The risk associated with a consignment may lead to a determination that armed escorts are required in non-operational settings. If armed escorts are required, AFP, AFP-PS or state and territory police services should be used in preference to private contract guards. Australian Defence Force (ADF) members providing escorts should not be armed. For further information on the use of private contract guards refer to DSPF Control 75.1 - *Contracted Security Guards*.

Police Escorts

14. It is recommended that civilian police escorts be used in addition to regular Defence escorts for transporting EO assigned a confidentiality BIL of 5 (Extreme) or classified SECRET or above.

Case Study: *An Army officer is transporting security-protected equipment between two bases. After assessing the risk, she arranges for ADF members from her own unit to provide escorts with the most senior of them taking on the OIC role. However, if she determined through her assessment that the risk was too high, she might choose to arrange a police escort. In both cases, she ensures the escorts are aware of the risks and responsibilities outlined in the MSP.*

How to Escort

Written Escort Instructions

15. The issuing entity is to issue written security instructions to the escort. The written instructions are not to reveal the nature or classification of the security-protected asset.

16. Written escort instructions may be included in the MSP.

Escort Requirements

17. The number of escorts required increases depending on the number of cargo vehicles being used to transport a consignment. The number of escorts required is based on a 1:3 ratio, i.e. one escort per three cargo vehicles (or part thereof). Therefore, if there are more than three cargo vehicles there should be an escort for every subsequent multiple of three cargo vehicles (or part thereof). The escort for the rearmost group of vehicles should travel at the rear of the convoy in the escort vehicle.

18. Security-protected assets requiring an escort should only be transported in an Australian Government or Defence contractor vehicle. There are limited situations (e.g. when a Defence employee is traveling interstate, overseas, or out-of-area and an Australian Government vehicle is unavailable) in which specific security protected assets can be transported in private vehicles (e.g. personally-owned vehicles, taxis, and hire cars).

Note: *External service providers involved in the transportation of EO may be able to operate under the requirements detailed in Annex A to this Control – Escorting Requirements for Explosive Ordnance External Service Providers (refer paragraph 24).*

Escort Vehicle Requirements

19. Escort vehicles **must** be crewed by a driver and an escort.

20. In multi-vehicle convoys, radio communications **must** be provided to all vehicles and escorts.

21. If security-protected assets requiring an escort are to be transported on public roads (including bases with open access), there should be at least one escort vehicle when:

a. more than one cargo vehicle is used;

b. the following quantities are transported in a single cargo vehicle:

i. one or more items of large assets assigned a BIL of 4 (Extreme) or above (or classified SECRET and above);

Note: *Refer to DSPF Control 71.1 - Physical Transfer of Official Information, Security Protected and Classified Assets for identification of what types of assets should be transported rather than transferred, (i.e. not sent via SCEC-approved courier).*

ii. seven or more pistols or non-automatic shoulder-fired weapons;

iii. two or more automatic shoulder-fired weapons;

iv. 10 or more sub-calibre training aids capable of firing a projectile by means of a powder charge;

v. Defence weapon controlled repair parts corresponding to and of the same amount as the weapons listed above;

Note: *Some exceptions to escort vehicle requirements apply to personal-issue weapons (refer paragraph 23).*

vi. bulk EO (as defined in DSPF Control 79.1 - *Explosive Ordnance Security*); or

Note: *There may be a case where the amount of EO is less than 'bulk' but requires more than one vehicle for safety purposes. An example is mixed EO of different compatibility groups. Safety requirements are available in Defence Explosive Ordnance Publication 103.*

vii. single unsecured canopied cargo vehicle is used for transportation of any amount.

Note: *A canopied vehicle is considered vulnerable and not secure if the canopy is made from canvas or similar such 'soft' materials. Cargo vehicles with canopies that are rigid and lockable do not apply in this regard.*

22. The number of escort vehicles required increases dependent on the number of cargo vehicles used to transport a consignment. The number is based on a 1:10 ratio, one escort vehicle per 10 cargo vehicles (or part thereof). Therefore, if there are more than 10 cargo vehicles there should be an escort vehicle for every subsequent multiple of 10 cargo vehicles (or part thereof). The escort vehicle for the rearmost group of cargo vehicles should travel behind the rear cargo vehicle. It is recommended that unsecured canopied cargo vehicles within a convoy are followed directly by an escort vehicle.

Case study: *A facility holding Defence servers is closing down and a manager from Chief Information Officer Group (CIOG) is responsible for moving servers to a new site. The servers have a BIL of 4 (Extreme) and will easily fit into two cargo vehicles. Since the journey is short and in a well policed area, he determines that contracted guards would be suitable for this activity. There are fewer than 10 cargo vehicles, so only one escort vehicle is required.*

Personal-issued Weapons

23. Where an individual or a small group of no more than six people is travelling with no more than two personal issued, non-bladed weapons each (e.g. a rifle and a pistol) there is no requirement for an escort vehicle; however there **must** be an escort designated who is not the driver of the vehicle.

EO External Service Provider Transport Operations

24. Where an external service provider has the following measures in place, it may follow the requirements detailed in Annex A to this Control - *Escorting Requirements for Explosive Ordnance External Service Providers* for the escorting of EO in lieu of the requirements above:

a. It **must** be Defence Industry Security Program (DISP) accredited and maintain compliance with the Australian Code for the Transport of Explosives by Road and Rail (AEC) and the Explosives Transport Regulations 2002 (ETR);

b. It **must** have cargo vehicles installed with satellite tracking and duress alarm systems for Category 2 or higher risk loads;

c. It **must** have inter-vehicle communications within a vehicle convoy in accordance with the AEC 3;

d. It **must** have communications to the base EO depot for Category 1 loads and higher risk loads;

e. It **must** have secure cargo areas in accordance with the AEC; and

f. It **must** have appropriate security clearances in place for its staff (refer DSPF Control 79.1 - *Explosive Ordnance Security*).

Note: *AEC Chapter 2 provides information of the different categories of EO.*

Roles and Responsibilities

Commanders and Managers

25. Commanders and Managers are responsible for ensuring that people nominated to escort security-protected assets have the necessary security clearances and training, and are fully briefed on their responsibilities and their response in the event that the shipment comes under attack, items are lost or stolen, or unauthorised access occurs.

Contract Managers

26. In instances where a MSP identifies the need for a licensed security guard to act as an escort, Defence contract managers are responsible for ensuring that contracts with external service providers require that the security guards are licensed in accordance with the relevant state and territory private security guard legislation and DPSF Principle 75 - *Contracted Security Guards*.

The Issuing Entity

27. The issuing entity is responsible for the security of the consignment in accordance with this DSPF part until the gaining entity takes possession.

28. The issuing entity is responsible for:

a. providing appropriately qualified numbers of escorts for the assignment;

b. ensuring that people nominated as escorts have the necessary security clearances and training;

c. providing adequate communications between all parties associated with the transportation (e.g. drivers, escorts and gaining entities) to enable communication in circumstances involving time delays, accidents or other incidents while in transit;

d. briefing the escort party on the MSP and other orders;

e. making all escorts aware of their legal powers of arrest unless those escorts are AFP, state or territory police officers or AFP-PS officers; and

f. obtaining a signed statement from each member of the escort party indicating that they fully understand their responsibilities.

Escorts

29. Escorts, who are escorting security-protected assets, are responsible for:

a. executing the MSP;

b. reasonably preventing unauthorised access to the consignment;

c. where physically possible, remaining with and observing the consignment at all times;

d. guarding the consignment during halts in the journey;

e. making parking arrangements with the nearest Defence authority or civilian police during night halts, extended halts or breakdown;

f. exercising appropriate powers in the protection of life and property, including powers of arrest if necessary;

g. maintaining a chronological log of events including:

   i. time of arrival and departure;

   ii. stop-over points;

   iii. transhipment points;

   iv. security arrangements at each stop;

   v. any security incidents that occurred; and

h. providing the log of events to the issuing entity after delivery of the escorted items.

Key Definitions

30. **Hand Carriage**. The personal carriage of classified information or security-protected assets by Defence personnel or external service providers who have the required security clearance to hold the information or asset.

31. **Escorts**. Civilian police officers, ADF members, APS employees or external service providers who guard or secure a load or consignment from theft, vandalism, sabotage or espionage. An escort may be armed or unarmed and does not drive escort or cargo vehicles, except in an emergency.

32. **Escort Vehicles**. Vehicles used in addition to cargo vehicle(s) in order to provide increased vigilance and protection.

33. **Cargo Vehicles**. Vehicles that are actively carrying a load of security-protected assets, including weapons and explosive ordnance.

34. **Security-protected Asset**. A non-financial, reportable or accountable information or asset that requires greater than standard fire and theft protection due to either:

a. being allocated a national security classification or Dissemination Limiting Marker (DLM);

Note: *The application of a security classification or DLM indicates that the information or asset has inherent confidentiality requirements.*

b. an unacceptable business impact that would result from the unauthorised modification (i.e. loss of integrity) of the information or asset, irrespective of whether that modification can be detected or not;

c. an unacceptable business impact that would result from the information or asset being unavailable (i.e. loss of availability) for a given period of time; or

d. being categorised as a weapon or explosive ordnance.

35. **Movement Security Plan** (MSP). A set of security measures detailed for the transport of security-protected assets, including weapons and explosive ordnance. A single MSP can be used to cover periodic movement of security-protected assets between the same parties, at non-changing departure and destination points (refer DSPF Control 71.1 - *Physical Transfer of Information and Assets*).

36. **Issuing Entity**. The Commander or Manager of a military or business unit, or authorised external service provider, responsible for issuing security-protected assets to a gaining entity.

37. **Gaining Entity**. The Commander or Manager of a military or business unit, or authorised external service provider responsible for taking possession of security-protected assets from an issuing entity.

Further Definitions

38. Further definitions for common PSPF terms can be found in the Glossary.

39. Definitions for common Defence administrative terms can be found in the Defence Instruction – Administrative Policy.

Annexes and Attachments

Annex A – *Escorting Requirements for Explosive Ordnance External Service Providers*

Document administration

Identification

DSPF Control	Escorting Security Protected or Classified Assets
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)
DSPF number	Control 81.1
Version	1
Publication date	2 July 2018
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	81
Related DSPF Control(s)	Physical Transfer of Official Information, Security Protected and Classified Assets Physical Security Contracted Security Guards Security Incidents and Investigations Weapons Security Explosive Ordnance Security Security of Radioactive Sources

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 SPS	Launch

Defence Security Principles Framework (DSPF)

Annex A to Escorting Requirements for Explosive - Ordnance External Service Providers

Process

1. This Annex is to be read in conjunction with the Australian Code for the Transport of Explosives by Road and Rail (AEC). The requirements detailed herein for the security of Explosive Ordnance (EO) only apply to external service providers that meet the requirements of DSPF Control 81.1 - *Escorting Security Protected or Classified Assets*, paragraph 9, which introduces this Annex.

Security Clearance

2. Security clearance requirements associated with EO are detailed in DSPF Principle 79 - *Explosive Ordnance Security*. Additionally, at a minimum, an Explosive Ordnance Outsourced Service Provider (EO OSP) Escort must have a BASELINE security clearance.

Requirements for Escorts and Escort Vehicles

3. Table 1 outlines the requirements for Escorts and escort vehicles in support of the risk categories of the loads being moved by an EO OSP. For certain loads the Load Supervisor is the sole Escort. Table 1 describes the movement for a single cargo vehicle. Within the table, Escort (ES) and Escort Vehicle (EV) refer to whether Escorts (additional to the Load Supervisor) or escort vehicles respectively are required

Table 1 – Escorted and escort vehicle requirements for a single cargo vehicle

Risk Category	ES – Retail Short	EV- Retail Short	ES – Retail Long	EV – Retail Long	ES – Retail Overnight	EV – Retail Overnight	ES - Wholesale	EV - Wholesale
Category 1	No[(a)]	No	No[(a)]	No	Yes	Yes	Yes	Yes
Category 2	No[(a)]	Yes[(b)]	No[(a)]	Yes[(b)]	Yes	Yes	Yes	Yes
Category 3	No[(a)]	Yes[(b)]	No[(a)]	Yes	Yes	Yes	Yes	Yes
High security risk	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes
Useful to the ill-disposed (UID) items[(c)]	No[(a)]	Yes[(b)]	Yes	Yes	Yes	Yes	Yes	Yes

Notes:

(a) The load supervisor is the escort

(b) An additional escort is not required to accompany the Driver in the escort vehicle

(c) Defined in Table 2

Movement Security Plans and Road Movement Orders

4. In accordance with DSPF Control 81.1 - *Escorting Security Protected or Classified Assets* the issuing authority (in this case the EO OSP) will develop appropriate Movement Security Plans (MSPs) in support of distribution activities. MSPs must be used for all movements.

5. A Road Movement Order (RMO) is only required as notification to both the police and the Defence Security & Vetting Service for overnight or wholesale distribution activities by the EO OSP or subcontractors. A RMO should be submitted 24 hours prior to the distribution event to the relevant police service and the DS&VS on the route of the distribution event.

Roles and Responsibilities

Explosive Ordnance Outsourced Service Provider

6. The EO OSP (and distribution subcontractors) is required to provide a Load Supervisor and a Driver in support of all EO distribution activities. The EO OSP may be required to provide an Escort as additional support to the Load Supervisor and

Driver depending on the risk category under which any particular load falls refer to Table 1 for further information.

Load Supervisor

7. The Load Supervisor, is responsible for:

a. implementing the MSP and RMO (if applicable) for the activity;

b. briefing all Drivers and Escorts (if required) on the MSP/RMO;

c. maintaining communications between the issuing/gaining entity, EO OSP depot and cargo/escort vehicles (as appropriate);

d. enacting emergency response requirements;

e. reporting and maintaining a log of unusual occurrences and providing it to the EO OSP security officer;

f. liaising with state and territory police services during retail overnight or wholesale distribution events in accordance with the RMO or for the use of armed Escorts;

g. monitoring the competence of the Driver(s) and Escort(s) in the performance of their duties;

h. coordinating and participating in the guarding of the consignment;

i. driving a vehicle if required; and

j. acting as an Escort if required (refer to Table 1 for such occasions).

Note: *The Load Supervisor is also the EO OSP issuing entity.*

Driver

8. In addition to the requirements detailed in the AEC, the Driver is responsible for:

a. monitoring the load and vehicle security;

b. adherence to the MSP and RMO (if applicable);

c. participate in the guarding of the consignment;

d. maintaining communications with the Load Supervisor, and

e. reporting unusual occurrences to the Load Supervisor.

Escort

9. The Escort's responsibilities are detailed in DSPF Control 81.1- *Escorting Security Protected or Classified Assets*.

Key definitions

10. **Retail Short**. EO OSP activities involved in the delivery or collection of EO to/from a Defence issuing or gaining entity within approximately a 100km radius of an EO OSP managed EO depot.

11. **Retail Long**. EO OSP activities involved in the delivery or collection of EO to/from a Defence issuing or gaining entity greater than 100km radius of an EO OSP managed EO depot.

12. **Retail Overnight**. EO OSP activities involved in the delivery or collection of EO to/from a Defence issuing or gaining entity where the EO OSP will require one or more overnight stopovers whilst on route.

13. **Wholesale**. EO OSP activities involving the redistribution of EO inventory between EO OSP managed EO depots using AEC-compliant long-haul subcontractors.

14. **Categories 1, 2 and 3**. The risk category assigned to a load of explosives, relating to low (1), medium (2) and high (3) risk and defined within AEC Chapter 2 (Risk Categories for Explosives table).

15. **High Security Risk Load**. A load of explosives described in AEC Chapter 2, which due to the combination of type and quantity is considered high risk for the purposes of security.

16. **Useful to the ill-disposed Items**. The term useful to the ill-disposed (UID) describes items, and the quantity thereof, that may be attractive to individuals seeking to use them for unauthorised purposes. These items are presented in Table 2.

Table 2 – Useful to the ill disposed items

Item	Quantity
Rocket 66mm	> 1
Mine Anti-personnel M18	> 6
Grenade Hand Fragmentation	> 12
Standard demolition kits	≥ 3 kits

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Escorting Requirements for Explosive Ordnance External Service Providers
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control 81.1).
DSPF Control	Escorting Security Protected or Classified Assets
DSPF Number	81.1

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 SPS	Launch

Defence Security Principles Framework (DSPF)

Procurement

General principle

1. Project Managers and Contract Managers are to ensure entities, to which Defence has granted access to official information or assets, take appropriate security measures to safeguard the information or assets. Security is to be considered and planned for throughout all stages of the procurement process.

Rationale

2. The procurement of goods and services has the potential to render Defence vulnerable to increased security threats and risks as contractors:

a. become knowledgeable about Defence capabilities through involvement in Defence projects;

b. are granted access to Defence bases and facilities, official information and assets, and Information and Communications Technology (ICT) systems; and

c. provide security-related goods or services.

Expected outcomes

3. Security risks are not outsourced, and remain with the Defence Group or Service responsible for the procurement activity.

4. Project Managers and Contract Managers manage the security risks that result from allowing contractors, and their subcontractors, access to Defence bases and facilities, official information and assets, and ICT systems.

5. Security risks associated with procurement activities are considered, assessed and managed in accordance with the DSPF.

6. The appropriate level of Defence Industry Security Program (DISP) membership is obtained and maintained, where required.

7. Defence Groups and Services ensure applicable security obligations contained in the DSPF are specified in contracts.

8. Appropriate strategies are established for the transition of security arrangements prior to the completion or termination of contracts.

Note: *A reference to contracts includes standing offers and panel arrangements.*

Escalation Thresholds

Risk Rating	Responsibility
Low	Assistant Secretary Materiel Procurement Branch (AS MPB)
Moderate	AS MPB
Significant	First Assistant Secretary Procurement and Contracting (FAS P&C)
High	Defence Security Committee (DSC) – through FAS P&C
Extreme	DSC – through FAS P&C

Note: *The DSPF Security Requirements have been incorporated into Defence's procurement policy framework and need to be incorporated in all contracting and procurement templates. Incorporation of security requirements into contracting templates/suites is the responsibility of the areas responsible for the template/suite, in accordance with the policy.*

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Procurement
Principle Owner	First Assistant Secretary Security & Vetting Service (FAS S&VS)
DSPF Number	Principle 82
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	None
Control Owner	Assistant Secretary Materiel Procurement Branch (AS MPB)

Related information

Government Compliance	**PSPF Core Requirements**: Eligibility and security of personnel; Access to information; and Security governance for contractors.
Read in conjunction with	Commonwealth Procurement Rules (CPRs) Defence Procurement Policy Manual
See also DSPF Principle(s)	Classification and Protection of Official Information Security for Projects Security for Capability Planning Foreign Release of Official Information Defence Industry Security Program Information Systems (Physical) Security ICT Certification and Accreditation Personnel Personnel Security Clearance Physical Transfer of Information and Assets Physical Security Certification and Accreditation Contracted Security Guards Security Incidents and Investigations Weapons Security Explosive Ordnance Security
Implementation Notes, Resources and Tools	***Note:*** *From 1 July 2018, existing contracts may be subject to a 12-month Transition Period during which the DSM will continue to apply as the authoritative statement of Defence security policy. Refer to Annex A of this DSPF Principle and the Contracts Review Process Guide for further information.* Australia National Audit Office, Better Practice Guide, Developing and managing contracts Australian Government, Contracting, Security of outsourced services and functions guidelines Commonwealth Procurement Rules (CPRs) Defence Procurement Policy Manual CASG Security Procurement and Contracting Tools and Templates Procurement and Contracting Help Desk Support

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

Defence Security Principles Framework (DSPF)

Annex A to Procurement – Transition Period

Transition Period Following Launch of the Defence Security Principles Framework

1. From 1 July 2018, Contracts may be subject to a Transition Period during which the Defence Security Manual (DSM) will continue to apply as the authoritative statement of Defence security policy.

2. The only Contracts subject to the Transition Period are those that (due to the original agreement, or due to extension of that agreement) extend for a term beyond 30 June 2018 and that:

a. refer specifically to the DSM;

b. contain bespoke security obligations;

c. involve security classified information or assets; or

d. are not subject to an agreed Contract Change Proposal (CCP) that requires compliance with the Defence Security Principles Framework (DSPF).

3. After 30 June 2019, all references in Contracts to the DSM are to be treated as references to current Defence security policy, including the DSPF.

Roles and Responsibilities

Contract managers

4. Contract Managers are to review all contracts (for which they are responsible) in line with the Capability Acquisition and Sustainment Group (CASG) *DSPF Contract review Process Guide*.

5. Contract Managers must ensure:

a. that from 1 July 2018 all contracts with contractors that are not subject to the Transition Period are subject to the security policy requirements of the DSPF.

b. That from 1 July 2019 all contracts with contractors are subject to Defence's current security policy requirements, including those in the DSPF.

Key definitions

6. **Transition Period**: The Transition Period will commence at midnight on 30 June 2018, and will continue until Midnight on 30 June 2019. During this time, applicable contracts may continue to operate with reference to the DSM.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Transition Period
Annex Version	1
Annex Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Principle).
DSPF Principle	Procurement
DSPF Number	Principle 82

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

Defence Security Principles Framework (DSPF)

SAFEBASE Security Alert Level System

General Principle

1. The SAFEBASE Security Alert Level System communicates threats of violent acts on Defence bases, sites and establishments (herein referred to as bases) and is underpinned by effective security planning.

Rationale

2. Acts of violence from terrorism, politically or issue-motivated groups and maverick individuals pose a threat to Defence's people and assets. It is important that Defence informs people on Defence premises of expected threats to support their decisions about security and safety.

3. Understanding and communicating changes to assessed violent threats operates alongside and enhances other DSPF Principles and Controls. Changes to SAFEBASE alert levels may be employed as an agile risk mitigation method which contributes to protecting Defence's people and assets.

Expected outcomes

4. SAFEBASE alert levels are escalated based on threat advice and risk assessments locally (single bases), regionally, or nationally.

5. SADFO, Base Managers and Heads of Resident Units effectively communicate Security Alert Levels to people on their bases.

6. SAFEBASE alert levels are time-bound and reviewed for appropriateness.

7. Defence's SAFEBASE alert levels support and enable security measures that:

a. can be implemented within the timeframes expected under the relevant alert level;

b. are cost-effective, appropriate to the local context, and can be effected within a base's existing resources;

c. focus on protecting against the threat at hand underpinned by localised, effective security risk management and up to date base security plans; and

d. ensure the base's core business can continue as required.

8. Roles and responsibilities at each SAFEBASE alert level have been communicated to Defence personnel, contractors, consultants and outsourced service providers on Defence premises and align with the *Joint Framework for Base Accountabilities*.

Escalation Thresholds

Note: *Security risk in the DSPF is usually escalated through the risk escalation thresholds. However, this DSPF Principle has no escalation thresholds. Security risk is to be managed in accordance with the Joint Framework for Base Accountabilities and through the application of DSPF Principles and Controls.*

SAFEBASE – Alert Level Escalation Thresholds

Level	Authority to raise or lower at a local base	Authority to raise or lower at the regional level	Authority to raise or lower at the national level
Aware	Chief Security Officer SADFO	Chief Security Officer	Chief Security Officer
Alert	Chief Security Officer SADFO	Chief Security Officer	Chief Security Officer
Act	Chief Security Officer SADFO	Chief Security Officer	Chief Security Officer

Note: *The Chief Security Officer is authorised to override a SADFO's changes to a base's alert level.*

Document administration

Identification

DSPF principle	SAFEBASE Security Alert Level System
Principle Owner	First Assistant Secretary Security and Vetting Service
DSPF Number	Principle 83
Version	2
Publication date	25 March 2019
Releasable to	Defence and Defence industry
Underlying DSPF Control(s)	Control 83.1
Control Owner	Assistant Secretary Security Policy and Services

Related information

Government Compliance	**PSPF Core Requirements:** Security planning; Security guidance for contracted service providers; and Entity physical resources. **Legislation**: *Defence Act 1903* *Workplace Health and Safety Act 2011* (Cth)
Read in conjunction with	Joint Framework for Base Accountabilities OPLAN SNAVE
See also DSPF Principle(s)	Counterintelligence Physical Security Physical Security Certification and Accreditation Access Control Contracted Security Guards Identification, Search and Seizure Regime Weapons Security Explosive Ordnance Security

Implementation Notes, Resources and Tools	• Australian Government physical security management protocol: https://www.protectivesecurity.gov.au/ • DS&VS security risk literature and planning tools via the Security Toolkit • Security Equipment Guides (SEGs) via the Security Toolkit. • ASIO Tech Notes via the Security Toolkit. • Security Equipment Evaluated Product List (SEEPL). This list contains products endorsed by the Security Construction and Equipment Committee (SCEC). • Contact 1800DEFENCE, your Executive Security Authority (ESA), or your DS&VS regional office for further information.

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	25 March 2019	FAS S&VS	SAFEBASE redesign system: simplified to three alert levels; additional customisation options; and clarification of authorities and notification responsibilities.

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

SAFEBASE Security Alret Level System

Control Owner

1. The Assistant Secretary Security Policy and Services (AS SPS) in the Defence Security & Vetting Service (DS&VS) is the owner of this enterprise-wide Control.

Escalation Thresholds

Note: *Security risk in the DSPF is usually escalated through the risk escalation thresholds. However, this DSPF Control has no escalation thresholds. Security risk is to be managed in accordance with the Joint Framework for Base Accountabilities and through the application of DSPF Principles and Controls.*

SAFEBASE – Alert Level Escalation Thresholds

Level	Authority to raise or lower at a local base	Authority to raise or lower at the regional level	Authority to raise or lower at the national level
Aware	Chief Security Officer SADFO	Chief Security Officer	Chief Security Officer
Alert	Chief Security Officer SADFO	Chief Security Officer	Chief Security Officer
Act	Chief Security Officer SADFO	Chief Security Officer	Chief Security Officer

Process

Overview

2. Every Defence base, site and establishment (referred to herein as base) in Australia is to use Defence's Security Alert Level system, SAFEBASE. The system consists of three levels:

(1) *Aware* (yellow): Threat advice of a violent act against Defence bases is generalised. No specific time or location is notified.

(2) *Alert* (orange): Threat advice indicates a specific timeframe for a violent act against specific bases.

(3) *Act* (red): A violent act on the base is either happening or imminent.

3. Changes to SAFEBASE alert levels may apply locally (to a single base), regionally (to a number of bases in a predefined geographic region) or nationally (Defence-wide).

4. Senior Australian Defence Force Officers (SADFOs) and Base Managers (BMs) should ensure SAFEBASE alert levels are communicated appropriately to people on their base to warn them of the threat, as well as, security plans and procedures.

Example: *Bases may communicate these messages through the use of signage, email alerts, or established Base Warning Alert Systems.*

Note: *for the purposes of SAFEBASE, Site Managers will have SADFO responsibilities at bases where no SADFO is appointed.*

5. Additional guidance on SAFEBASE levels can be found on the DS&VS Security Portal Intranet Page.

Authority to Raise and Lower the Alert Levels

6. The Chief Security Officer, or an approved delegate, is authorised to set the SAFEBASE alert level at the national, regional or local level in response to threat and risk assessments.

Note: *The First Assistant Secretary Security and Vetting Service (FAS S&VS) is the Chief Security Officer.*

7. SADFOs are authorised to set the SAFEBASE alert level at the local level only (their local base) in response to security threat and risk advice.

8. SADFOs **must** acknowledge and act on Chief Security Officer-authorised changes to relevant alert levels.

Note: *There may be restrictions that prevent the complete dissemination of threat information (such as operational considerations, classifications or handling caveats). When authorising the change of alert level, the Chief Security Officer will aim to provide as much actionable information as possible and clear instructions on any dissemination limitations.*

Raising Levels

9. Decisions to change SAFEBASE alert levels should be threat-based and informed by consultation with intelligence and law enforcement agencies, Headquarters Joint Operations Command (HQJOC), and local base authorities.

10. Decisions to raise a base's alert level from *Aware* to *Alert* should be based on credible threat intelligence that:

a. the base will be the target of a violent act; and

b. the violent act is expected within a specific timeframe (for example, within a week or a month).

11. Decisions to raise a base's alert level to *Act* should be based on credible threat intelligence that:

a. a violent act is currently happening on the Defence base; or

b. a violent act against the base is imminent, based on advice from DS&VS, the Chief Security Officer, intelligence and law enforcement agencies, or HQJOC.

Lowering Levels

12. The Chief Security Officer is authorised to de-escalate a SAFEBASE alert level nationally, regionally and locally.

13. The Chief Security Officer is authorised to override a SADFO-authorised alert level.

14. SADFOs can de-escalate at the local level when a threat is no longer apparent, or on resolution of an incident, and **must** notify the HQJOC Joint Operations Room (JOR) within six hours.

SAFEBASE Level Requirements

15. Security Management Plans should include plans for each SAFEBASE alert level, and should be developed in accordance with the *Joint Framework for Base Accountabilities* (JFBA) (including Emergency Response Plans and Base Continuity Plans), and OPLAN SNAVE.

Note: *OPLAN SNAVE describes the broader ADF response plan to counter either a no-warning armed domestic attack on, or emerging potential threat against, Defence bases.*

Aware level

16. At the *Aware* level:

(1) Defence is receiving generalised intelligence with no specific indication of an act against any particular Defence base.

(2) DS&VS disseminates threat advice as appropriate, and operations at Defence bases are expected to continue as usual.

Case Study: *DS&VS has received generalised threat advice from Australian intelligence agencies. A terrorist attack remains probable, but no intelligence of a specific time or location has been received.*

Alert levels remain at Aware. DS&VS disseminates its threat advice to bases to inform security risk management. Based on this advice, BMs review and adjust, in consultation with SADFOs, security management plans to mitigate security risks. Minor incidents are resolved without the need to elevate the alert level.

Normal business operations continue. Base planning prepares staff and emergency control personnel to respond to a violent security incident.

Alert level

17. At the *Alert* level:

(1) The SADFO makes a decision to take command of the base in accordance with the JFBA, and additional protective measures are activated in accordance with the Base Security Plan.

(2) Upon elevating the alert level, the SADFO must notify the HQJOC JOR immediately. HQJOC may decide to enact OPLAN SNAVE.

(3) HQJOC JOR will coordinate with and notify other stakeholders, including the Chief Security Officer.

(4) The Chief Security Officer will review the alert level weekly.

(5) Affected bases operate at higher alert levels with expected limitations on business and operations.

Case Study: *The SADFO of a RAAF base in Queensland has been informed of planned protests on public grounds outside the base. Protests have been held without issue outside this base previously and protest organisers have coordinated their activities with the local authorities.*

However, in consultation with local law enforcement, the SADFO learns that some members of this protest group have been violent at past protests at other Defence bases.

The SADFO decides to raise the alert level to Alert, assumes command in accordance with the JFBA and enacts plans to mitigate the risk of violence against Defence personnel. For this specific base, this includes increased patrols, increased security awareness communications, and the locking of nonessential access points.

The SADFO alerts HQJOC JOR of the elevated alert level. HQJOC JOR notifies all key stakeholders, including the Chief Security Officer, and monitors the situation.

The base continues to operate at an alert level of Alert until the protest ends. After reviewing the situation, the SADFO returns the base to an Aware level and notifies HQJOC JOR.

Act level

18. At the *Act* level:

(1) the SADFO makes a decision to take command of the base in accordance with the JFBA and activates emergency responses and procedures.

(2) the SADFO **must** notify and coordinate with local law enforcement authorities upon elevation. Civilian police have primacy.

(3) the SADFO **must** alert and coordinate with the HQJOC JOR as soon as reasonably practicable and OPLAN SNAVE may be enacted by HQJOC.

(4) HQJOC JOR will coordinate with and notify other stakeholders, including the Chief Security Officer.

(5) The Chief Security Officer will review the alert level every 48 hours.

(6) The *Act* level should be maintained for as long as the violent act is underway or expected to be imminent. It is expected that this alert level is sustained for no longer than 48 hours.

Case Study: *The Australian Federal Police (AFP) have just disrupted a terrorist cell in a city in New South Wales, which had been planning to attack a Defence base in the nearby region. Defence's Chief Security Officer is informed that the AFP was able to arrest most of the cell's leaders, but has reason to believe some of its members escaped.*

After receiving this threat advice, the Chief Security Officer instructs SADFOs in the nearby region to raise their base's alert level to Alert. Local SADFOs communicate the increased threat to base personnel and implement additional security measures in accordance with their security management plan.

The next day, four unauthorised persons enter one of the bases and ignore instructions from the contracted guards. They are carrying backpacks and the guards are concerned that they may contain weapons.

In response, the SADFO contacts local law enforcement in accordance with the base's emergency plans and raises the SAFEBASE level to Act. The SADFO then notifies HQJOC JOR. Emergency Services arrive at the scene shortly.

While the SADFO is overseeing emergency procedures, HQJOC JOR notifies key stakeholders, including Defence's Chief Security Officer. The Chief Security Officer liaises with the intelligence and law enforcement agencies to assess the ongoing threat.

Local law enforcement are able to quickly resolve the situation and all intruders are now in custody. There is no longer a direct threat and the SADFO decides to lower the alert level to Alert, and notifies HQJOC JOR.

Updated threat advice from the intelligence and law enforcement agencies convinces the Chief Security Officer that there is no further specific threat of violence against bases in the region. The Chief Security Officer instructs regional bases to lower their SAFEBASE levels to Aware.

Assurance requirements

19. The Chief Security Officer will report on all instances of alert level elevations to the Secretary and Chief of Defence Force.

20. SADFOs and BMs are to report on all security incidents that arise during elevated alert levels, in accordance with DSPF Principle 77 – *Security Incidents and Investigations*.

21. SADFOs and BMs should regularly review their base security plans, exercises, and emergency incident response plans in accordance with the JFBA.

Document administration

Identification

DSPF Control	SAFEBASE Security Alert Level System
Control Owner	Assistant Secretary Security Policy and Services (AS SPS)
DSPF Number	Control 83.1
Version	2
Publication date	25 March 2019
Type of Control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Defence Security Alert Level System
Related DSPF Control(s)	Physical Security Physical Security Certification and Accreditation Access Control Contracted Security Guards Identification, Search and Seizure Regime Weapons Security Explosive Ordnance Security

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 SPS	Launch
2	25 March 2019	AS SPS	SAFEBASE redesign system: simplified to three alert levels; additional customisation options; and clarification of authorities and notification responsibilities

Defence Security Principles Framework (DSPF)

Fuel Security

General principle

1. Bulk petroleum fuel must be secured from theft, loss or unauthorised access.

Rationale

2. Bulk fuel, because of its flammability, has the capacity to cause large fires and explosions presenting significant risks to people, the environment and capability assurance. Tampering with fuels storage and handling equipment by untrained persons can result in such risk being realised. In addition, fuel is a valuable commodity and is known to be targeted for theft by unscrupulous organisations or individuals. Systematically managing the security risk environment for Defence Fuel Installations and Defence Fuel Supply Chain (DFSC) activities provides a secure environment in which operations may be successfully and safely conducted. Additionally, it assures Defence fuel stocks and associated plants are protected from unauthorised actions.

Expected outcomes

3. DFSC workers, including authorised visitors and contractors, are protected from security related risks associated with external threats.

4. Access to Defence bulk fuel sites, facilities and/or fuel supply chain vehicles is controlled in accordance with prescribed internal and external (legislative) requirements.

5. Defence property within the DFSC (including intellectual property and data) is protected from harm or loss.

6. Fuel operations within the DFSC comply with all requirements of Defence Security policy.

7. Defence personnel, Contractors, Consultants and Outsourced Service Providers are fully compliant with the *Defence Fuels Management System (DFMS) Element 11.0: Security Management*.

Escalation Thresholds

Risk Rating	Responsibility
Low	APS6 / O4 or equivalent in relevant Group / Service
Moderate	EL1 / O5 or equivalent in relevant Group / Service
Significant	Director General (DG) / EL2 / O6 or equivalent in relevant Group / Service
High	Defence Security Committee (DSC) via Commander Joint Logistics (CJLOG)
Extreme	DSC via CJLOG

Note: *Contractors, Consultants and Outsourced Service Providers are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Fuel Security
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 84
Version	1
Publication date	2 July 2018
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	N/A
Control Owner	Commander Joint Logistics

Related information

Government Compliance	**PSPF Core Requirements**: Entity physical resources and Entity facilities. **Legislation**: The following legislation always applies. • *Work Health and Safety Act 2011* • *Work Health and Safety Regulations 2011* • *Environment Protection and Biodiversity Conservation Act 1999* *In specific circumstances the following can also apply;* • *Aviation Transport Security Act 2004* • *Maritime Transport and Off-shore Facilities Security Act 2003* • *Specific Airports Acts and Regulations;* • *Specific Ports and Marine Environment management legislation;* • *The Australian Code for the Transport of Dangerous Goods by Road and Rail* • *State based Pipelines management legislation*
Read in conjunction with	All policy and procedures as prescribed by single Service requirements (Navy, Army or Air Force as applicable) in relation to security of Defence assets and activities. All Elements of the DFMS in relation to the safe handling of fuel.
See also DSPF Principle(s)	Personnel Security Clearance Temporary Access to Classified Information and Assets Identity Security Physical Security Certification and Accreditation Access Control Security Incidents and Investigations
Implementation Notes, Resources and Tools	Defence Fuel Management System - Element 11.0: Security Management

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