Australian Government
Defence

DEFENCE SECURITY PRINCIPLES FRAMEWORK

Peter West
Chief Security Officer
First Assistant Secretary
Defence Security Division
Policy Owner (Security)

Department of Defence
CANBERRA ACT 2600

19 July 2024

Contents

Principle 16
Defence Industry Security Program
Control 16.1
Defence Industry Security Program

- Annex A to Defence Industry Security Program – DISP Membership Levels
- Annex B to Defence Industry Security Program – Resources and Contacts
- Annex C to Defence Industry Security Program - Special Access Programs

Principle 41
Temporary Access to Classified Information and Assets

Control 41.1
Temporary Access to Classified Information and Assets

Principle 44
Overseas Travel

Control 44.1
Overseas Travel

- Annex A to Overseas Travel – Overseas Travel Briefing and Debriefing Guides
- Annex B to Overseas Travel – Travelling with Portable Electronic Devices and Media

Principle 70
Working Offsite

Control 70.1
Working Offsite

Principle 72
Physical Security

Control 72.1
Physical Security

- Annex A to Physical Security – Security Containers, Vaults, and Safes
- Annex B to Physical Security – Policy Transition from Security Rated Areas to Physical Security Zones

Principle 73
Physical Security Certification and Accreditation

Control 73.1
Physical Security Certification and Accreditation

Principle 80
Radioactive Sources

Principle 84
Fuel Security

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 Accountable Authority for Defence.

2. This document and the related DSPF Principles and Controls have been issued by the **Chief Security Officer** with the authority of the Accountable Officer for Security – Deputy Secretary Security and Estate.

Note: *The First Assistant Secretary Defence Security (FAS DS) is the* ***Chief Security Officer*** *for Defence.*

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 persons engaged under a contract.

7. The Secretary and the Chief of the Defence Force (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*.

  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 persons engaged under a contract 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. **Deputy Secretary Security and Estate**, is the accountable officer for security.

16. The DSPF is a flexible policy framework. DSPF documents have been regularly reviewed and updated as necessary from the original publication date of 02 July 2018.

17. Authoritative DSPF documents are only available from the interactive DSPF site on the Defence Protected Network (DPN). A non-interactive version is also available from the DPN Defence manuals page. The currency of DSPF documents cannot be guaranteed if sourced from other locations.

18. The security advice function, including queries on the DSPF, is provided in the first instance through 1800DEFENCE. Additional information can be found on the DPN.

The structure of the DSPF

19. 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.

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

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

See DSPF Roles and Responsibilities Diagram

21. The Defence-specific guidance will be provided through a suite of documents that will reference the PSPF. The DSPF is the authoritative source for enterprise security policy in Defence.

22. The three tiers of Defence Guidance are:

- *DSPF Governance and Executive Guidance*: This document establishes and explains the DSPF.
- *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).
- *DSPF Enterprise-wide Controls*: Where necessary, these documents provide additional controls, processes and instructions relating to the interpretation and the application of *DSPF Principles and Expected Outcomes* 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* have accompanying *DSPF Enterprise-wide Controls*.

Understanding Principles and Expected Outcomes

23. *DSPF Principles and Expected Outcomes* 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).

24. *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

25. 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.

26. Each *DSPF Principles and Expected Outcomes* document contains a "See also" section and an "Implementation Notes, Resources and Tools" section to provide applicable external implementation guidance.

Understanding DSPF Enterprise-wide Controls

27. Where additional guidance is needed to manage or mitigate a security risk beyond the general principle provided in the *DSPF Principles and Expected* Outcomes documents, it may be appropriate to develop a *DSPF Enterprise-wide Controls* document which provides controls, processes and instructions.

28. *DSPF Enterprise-wide Controls* 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 63).

29. *DSPF Enterprise-wide Controls* 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 35).

30. **Control Owners** (refer paragraph 63) may set *DSPF Enterprise-wide Controls*. Subordinate security controls, processes and instructions may be Group or Service specific, collaborative or locational. These should be approved by the relevant **Control Owner**.

Security Controls Guidance

31. Subordinate 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, in accordance with Records Management Policy Manual and guided by the Good Administrative Decision-Making Manual.

Reviewing Controls, Processes and Instructions

32. *DSPF Enterprise-wide Controls*, and security decisions more broadly, may need to be reviewed; in line with continuous improvement and best practice. The requirement exists to review *DSPF Enterprise-wide Controls*, 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.

Review process

33. Areas undertaking a review of their DSPF Control or Principle are to provide all proposed updates to the Enterprise Security Policy (ESP) team for a quality check.

34. ESP will then progress the updates to FAS DS for review and approval.

Risk Management

33. 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.

34. Security risks are managed under the DSPF through:

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

Mandatory Provisions

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

36. Any mandatory provision under the DSPF is to be approved by the **Chief Security Officer**. The **Chief Security Officer** is authorised to establish mandatory provisions under the *Defence Instruction* and non-compliance is a reportable security incident.

37. Where it is determined that a departure from a mandatory provision is required, a dispensation may be sought from the relevant **Control Owner**. Dispensations can only be approved by the **Control Owner**.

Escalating and Accepting Risks

38. 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*. Persons engaged under a contract cannot manage or escalate risks except through Defence personnel.

39. 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 61).

40. 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).

41. With the exception of mandatory provisions, Defence personnel and persons engaged under a contract should regard *DSPF Enterprise-wide Controls* as guidance. Accepting the risk of departing from policy is to be guided by the escalation thresholds.

42. 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 the **Chief Security Officer** or the **Chief Information Security Officer** for review of impact on obligations to the Commonwealth.

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

44. 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 67) and **Control Officers** (refer paragraph 70) 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

45. The Secretary has an obligation to report annually to government on Defence compliance with the PSPF. The Secretary is assisted by the **Chief Security Officer,** who provides an enterprise-wide view of Defence's security risk to the **DSC**.

46. The enterprise-wide security risk view is underpinned by assurance reporting from **Control Owners** (refer paragraph 63). **Control Owners** are required to provide a biennial report to the **DSC** on implementation of each *DSPF Principle and Expected Outcomes* they have responsibility under by completing the DSPF Control Owner Reporting template. The purpose of this report is to:

- Provide general assurance to the **DSC** that a specific *DSPF Principle and Expected Outcomes* 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.

47. 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.

48. 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 *DSPF Enterprise-wide Control* to another. **Control Implementers** will provide appropriate assurance to **Control Owners** and escalate risks in accordance with defined thresholds.

Training and Awareness

49. 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.

50. To support a robust and positive security culture, Defence personnel and persons engaged under a contract are to undertake suitable security training through:

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

51. Further guidance regarding suitable security training can be obtained from the Defence Security intranet section.

Roles and Responsibilities

52. The Secretary is the Accountable Authority, in accordance with the Public Governance, Performance and Accountability Act. This role is expected to meet the four security outcomes of the PSPF through the Department of Home Affairs' 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, persons engaged under a contract and clients.

See DSPF Roles and Responsibilities Diagram

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

- The Associate Secretary as the chair of the **Enterprise Business Committee** (EBC).
- The Deputy Secretary Security and Estate as the chair of the **DSC**.
- Security issues will be escalated through the two committees.

- The FAS DS as the **Chief Security Officer**, is responsible for overseeing the development and implementation of the DSPF.

- The Director-General of the **Australian Signals Directorate** is the accreditation authority for TOP SECRET Sensitive Compartmented Information Facilities (SCIFs) and is the Communications Intelligence Security Authority for Defence.

Chief Security Officer

54. As the **Chief Security Officer** for Defence, FAS DS is delegated responsibility by the Secretary for Defence's security risk management.

55. In accordance with the PSPF, the **Chief Security Officer** is responsible for directing all areas of the Defence enterprise's security to protect Defence's people, information (including ICT) and assets.

56. This includes key oversight responsibilities outlined in the *PSPF Policy 2 – Management Structures and Responsibilities*.

57. Defence-specific responsibilities include:

- Supporting and advising the Secretary and Chief of the Defence Force on security matters in Defence;

- Maintaining and overseeing the DSPF, specifically:

    - maintaining the *DSPF Governance and Executive Guidance*;

    - the DSPF Principles and Expected Outcomes, except for ICT Principles and Expected Outcomes, which are managed by the **Chief Information Security Officer**;

    - appointing **Control Owners**;

- Maintaining and overseeing clear security accountabilities and reporting structures through the DSPF;

- Appointing security advisers in Defence in accordance with PSPF requirements. This includes the appointment of a **Chief Information Security Officer**, in consultation with the Chief Information Officer;

- Reporting on the risk and effectiveness of *DSPF Enterprise-wide Controls* to the **DSC**;

- Producing Defence's annual PSPF report for Secretary approval;

- Promoting and fostering a positive security risk management culture within Defence; and

- Directing security training, threat information dissemination, security awareness programs, and incident reporting and investigations in Defence.

Chief Information Security Officer

58. The **Chief Security Officer** has designated the Assistant Secretary Defence Cyber & Information Assurance Branch (DCAIB), Joint Capabilities Group (JCG), as the **Chief Information Security Officer** for Defence.

59. The **Chief Information Security Officer** is responsible for providing strategic level leadership, guidance and reporting for Defence's cyber security program to the **Chief Security Officer**.

60. This includes ensuring compliance with Whole-of-Government cyber security policy, standards, regulations and legislation.

Defence Security Committee

61. The **DSC** is chaired by the Deputy Secretary Security and Estate and reports to the Risk Owner via the **EBC**.

62. The **DSC** provides the primary oversight of the DSPF. **DSC** members:

- Provide security risk management and strategic direction;

- Address escalated residual security risks;

- Consider **Control Owner** (refer paragraph 63) and enterprise-wide security risk reports; and

- Seek to resolve any security related risks, problems or disagreements.

Control Owner

63. 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*. The relevant **Control Owner** in each instance may be a Group Head or Service Chief, or a more appropriate subordinate.

64. **Control Owners** will:

- Manage, monitor and report on the implementation across the Defence enterprise of any *DSPF Principles and Expected Outcomes*;

- Set relevant *DSPF Enterprise-wide Control*s;

- Approve subordinate security controls, processes or instructions for Group or Service specific, collaborative or locational purposes;
- Define **Control Implementers** (refer paragraph 67) and establish any necessary horizontal accountability arrangements, including oversight of subordinate 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*;
- Provide appropriate assurance and reporting to the **DSC** and the **Chief Security Officer**;
- 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).

65. **Control Owners** will be proposed to implement *DSPF Principles and Expected Outcomes* as required by the **Chief Security Officer** on the basis of:

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

66. Where a **Control Owner** cannot be agreed, the ownership will be referred to the **DSC** (refer paragraph 61).

Policy Owner and Publishing Authority

*While **Control Owners** are responsible for the setting of any* DSPF Enterprise-wide Controls*, the **Chief Security Officer** is the Policy Owner and the DSPF publishing authority. **Control Owners** must meet DSPF Principles and Expected Outcomes when developing variations to their DSPF Enterprise-wide Control. Further guidance can be obtained from the Directorate of Administrative Policy and the Policy Resources page.*

Control Implementer

67. 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 *DSPF Enterprise-wide*

Controls to mitigate or manage security risks. They will generally be the Managers or Commanders with some specific responsibility for the implementation of the *DSPF Enterprise-wide Control*.

68. **Control Implementers** will:

- Implement *DSPF Enterprise-wide Controls* within their business unit;
- If required, develop subordinate security controls, processes or instructions that are Group/Service specific, Collaborative or Locational (such as Standard Operating Procedures);
- If required, exercise delegated authority as directed by the **Control Owner**;
- 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**.

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

Control Officers

70. **Control Officers** encompass all staff and stakeholders in the Defence Enterprise. Defence personnel and persons engaged under a contract all have a duty to manage security risk in accordance with the DSPF.

71. Supervisors and custodians of information and assets are accountable for the appropriate implementation of *DSPF Enterprise-wide Controls* within their work places.

72. 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 persons engaged under a contract

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

73. 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

74. **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.

75. 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 Enterprise-wide Controls*.

76. Commanders and Managers are to appoint **Security Officers** wherever sensitive or classified information and/or security protected assets are stored or handled. They should be appropriately trained (see the Defence Security intranet section for current Security Officer training requirements) and hold an appropriate security clearance.

77. Commanders and managers are not to appoint an external service provider as a **Security Officer**.

Australian Government
Defence

DEFENCE CHIEF INFORMATION SECURITY OFFICER (CISO)

CHARTER

1. The role of the Chief Information Security Officer (CISO) is to provide strategic level leadership and guidance for Defence's cyber security program and ensuring compliance with whole of government cyber security policy, standards, regulations and legislation.

2. The CISO is an SES Band 1 officer within Joint Capabilities Group (JCG), appointed by the Chief Security Officer (CSO) with the endorsement of the Chief Information Officer as required under the Defence Security Principles Framework.

3. The CISO is responsible for providing cyber security related, whole of Defence strategic direction, reporting and advice to the CSO as required under the Defence Security Principles Framework.

Responsibilities:

4. The CISO is responsible to the CSO for:

a. ensuring that responsibilities, authorities and accountabilities in cyber security across Defence are clear and well defined;

b. developing and maintaining a Defence Cyber Security Strategy and associated Cyber Security Program, to ensure a consistent approach and effective delivery of Defence's cyber security capability;

c. providing cyber security performance reporting to meet Australian Government and Defence security assurance and compliance requirements, and enable effective cyber risk management and decision making for Defence;

d. Chairing and coordinating the quarterly meeting of the Cyber Security Governance Board to ensure cyber security investments, activities and risks are coordinated and effectively managed across the Defence Groups and Services;

e. maintenance of the Defence Security Principles Framework Principles and Expected Outcomes related to cyber/ICT security;

f. developing and promulgating an effective suite of whole-of-Defence cyber security policy, manuals, standards, patterns and guidance consistent with the Defence Security Principles Framework, Information Security Manual and best practice, including cyber supply chain risks;

g. advice and guidance on significant cyber security risks that contribute to Defence's overall security performance and agency level risk;

h. providing advice on cyber for major projects;

i. overseeing and ensuring coordination of the monitoring, detection and response to cyber vulnerabilities, threats and incidents for Defence;

j. contributing development, maintenance and exercising of incident response, business continuity and disaster recovery plans, leading cyber security components;

k. ensuring capability readiness to meet assigned obligations under CDF Preparedness Directive;

l. developing and implementing whole-of-Defence cyber security awareness and education activities;

m. ensuring implementation of appropriate structures to raise, train and sustain workforce associated with ICT Job Families - Cyber Security Function; and

n. managing the Cyber Security Accreditation function for Defence and delegating Accreditation Authority to the appropriate capability manager (as required).

Peter West
Chief Security Officer
First Assistant Secretary
Defence Security Division

29 May 2024

Jonathan Dean
Defence Chief Information
Security Officer (CISO)
Joint Capabilities Group

3 June 2024

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 information, according to the potential impact on the national interest, Government, organisations or individuals if the information were compromised.

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.

3. 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

4. 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. The security classification assessment will be informed by a broader assessment of Business Impact Levels (BILs) on each occasion.

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

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

Document administration

Identification

DSPF Principle	Classification and Protection of Official Information
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS DS)
DSPF Number	Principle 10
Version	4
Publication date	28 June 2024
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 Information Systems Data Transfer Security
Implementation Notes, Resources and Tools	Business Impact Levels Questions and Answers, 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 DS	Launch
2	31 May 2019	FAS DS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	28 June 2024	FAS DS	Control Owner review; PSPF alignment

Australian Government
Defence

Defence Security Principles Framework (DSPF)

Classification and Protection of Official Information

Control Owner

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

Escalation Thresholds

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

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

Introduction

3. This DSPF Control provides guidance on classification and protection of Official Information in Defence. This Control should be read in conjunction with Control 72.1 Physical Security and Control 21.1 Information and Technology Security (Physical).

4. Additional guidance for specific activities can be found in the Annexes of this DSPF Control.

5. To ensure Defence personnel and persons engaged under a contract are meeting the Expected Outcomes of DSPF Principle 10 – *Classification and Protection of Official Information*, the following mandatory provisions apply:

a. Official Information requiring increased protection **must** be clearly marked with the appropriate Protective Marking in accordance with the Australian Government Protective Security Policy Framework (PSPF).

b. Altering the Protective Marking on Official Information **must not** be done without Originator approval.

c. Official Information **must** be protected with suitable controls commensurate with its level of sensitivity and/or classification.

d. Official Information **must** only be released to, and accessed by, those who need-to-know the information for their official duties.

e. Classified information **must** only be released to, and accessed by, those who have the appropriate level of security clearance required and with a need-to-know.

f. Caveated information **must** only be accessed and handled in accordance with the relevant caveat controls in this DSPF Control.

g. Official Information **must not** be protectively marked in order to:

(1) hide violations of law, inefficiency or administrative error.

(2) prevent embarrassment to an individual, organisation or agency.

(3) restrain competition.

(4) prevent or delay the release of information that does not need protection in the public interest.

h. All Defence personnel **must** have agency authorisation to release any Official Information to members of the public. For further information, refer to Annex A of this DSPF Control.

i. Documents and Files containing information covered by more than one classification **must** be classified to the highest level of information contained within.

j. Classified information **must** be appropriately filed in accordance with the *Archives Act 1983* and the Defence Records Management Policy. Refer to Annex B of this DSPF Control.

k. All information classified TOP SECRET, and accountable material, held by Defence **must** be registered. Refer to Annex E of this DSPF Control.

l. All information classified SECRET and above, and accountable material, held by Defence Industry Security Program (DISP) members **must** be registered. Refer to Annex E of this DSPF Control.

m. Disposal of sensitive and classified information **must** be in accordance with Defence Records Management Policy and by methods appropriate for the level of classification in accordance with Whole of Australian Government requirements. Refer to Annex H of this DSPF Control.

n. Classified information **must** be transferred or transmitted by secure means commensurate with its level of classification. Refer to DSPF Principle 71 - *Physical Transfer of Information and Assets* or DSPF Principle 25 - *Information and Technology Security (Gateways & Data Transfers)*.

Protecting Official Information

6. Official information is all information created, sent or received as part of the work of the Australian Government, by Defence personnel and persons engaged under a contract in their professional capacity. This may include:

a. documents and paper;

b. data;

c. software or systems and networks on which the information is stored;

d. intellectual information (knowledge) acquired by individuals; and

e. physical items from which information regarding design, components or use could be derived.

7. Official Information encompasses sensitive and security classified information.

8. Defence personnel and persons engaged under a contract **must** take appropriate steps to ensure that Official Information is protected from compromise or unauthorised access in accordance with the information's Protective Marking.

Note: *The unauthorised disclosure of Official Information may be subject to the sanction of criminal law under* ***Part 5.6 of the Criminal Code 1995 (Cth)****.*

9. This applies to information in any form, including oral, written, electronic, documentary, visual, briefings, material and equipment.

Assessing Official Information

10. Originators are to determine the sensitivity of Official Information by assessing the damage that the information or asset would likely cause to Defence and/or the Australian Government if compromised. This is called assessing the Business Impact Level (BIL) (see Table 1).

11. The BIL determines if Official Information requires a routine level of protection, is sensitive or requires a security classification.

***Note**: The Originator is the functional position from which the information was originally prepared, not the individual who prepared the document.*

Table 1: Business Impact Levels

BIL	1 (Low)	2 (Low-Medium)	3 (High)	4 (Extreme)	5 (Catastrophic)
Protective Marking	OFFICIAL	OFFICIAL: Sensitive	PROTECTED	SECRET	TOP SECRET
Compromise of information confidentiality would be expected to cause:	**No or insignificant damage**. This is the majority of routine information.	**Limited damage** to an individual, organisation or government generally if compromised.	**Damage** to the national interest, organisations or individuals.	**Serious damage** to the national interest, organisations or individuals.	**Exceptionally grave damage** to the national interest, organisations or individuals.

12. Further guidance on how to assess the BIL of Official Information and how to apply the corresponding Protective Marking can be found in Annexes E and F of this DSPF Control.

13. Official Information should be protectively marked at the lowest level allowed through the assessed BIL. The appropriate use of Protective Markings enables Defence to engage internally and externally as necessary, subject to the need-to-know principle. The misuse of Protective Markings, including the over-classifying Official Information, inhibits information sharing and collaboration.

Limiting Access to Official Information

14. **Security clearance.** Defence personnel and persons engaged under a contract **must** ensure that access to Classified Information is limited to those who hold the appropriate level of security clearance. For further information refer to DSPF Principle 40 - *Personnel Security Clearance*.

15. **Need-to-know principle.** Defence personnel and persons engaged under a contract **must** ensure that access to Official Information is limited to those who need to know the information for their official duties.

Exclusion: *Official Information that has been formally approved for Public release is not subject to the need-to-know principle.*

Managing Official Information in Your Business Area

16. **Clear desk.** Defence personnel and persons engaged under a contract are responsible for the security of Official Information under their control. Defence personnel and persons engaged under a contract are to ensure that no protectively marked Official Information is left unattended at their workstation in order to prevent unauthorised access.

17. **Session and Screen Locking.** Defence Personnel and person/s engaged under a contract are to ensure their workstation screen is locked when unattended to ensure unauthorised access to Defence ICT systems and Official Information is deterred.

18. **Close of day checks.** At the close of business each day, Defence personnel and persons engaged under a contract are to take precautions to ensure that Official Information, especially sensitive or classified information, is protected from unauthorised access. It is recommended that Security Officers develop a workplace lock-up procedure which may include, but not be limited to the following:

a. Ensuring no sensitive or security classified information is left unattended on a desk (that is, it is stored appropriately).

b. Logging off all systems.

c. Ensuring desk are clear of documents to avoid sensitive or classified information being left out in the workplace.

d. Ensuring that laptops and other electronic media storing security classified information are secured.

e. Ensuring Official Information has been disposed of appropriately, including checking waste-paper bins.

f. Ensuring that whiteboards and other displays do not show any security classified information.

g. Ensuring vaults and containers are locked.

h. Ensuring windows and doors are locked.

i. Ensuring that container keys are secured.

j. Keys are not left in doors and drawers (at the end of the day or for an extended period of time).

19. It is also recommended that Commanders and Managers put in place an appropriate system for checking the workplace at close of business (or the end of shifts) to ensure that Official Information is secured appropriately.

Working Offsite

20. Requirements for offsite work are provided in DSPF Principle 70 – *Working Offsite* and Control 70.1 – *Working Offsite*.

Applying Protective Markings to Official Information

21. The Protective Marking of Official Information informs the level of protection afforded to it. Specific guidance on applying Protective Markings to Official Information can be found in Annexes E and F of this DSPF Control.

22. The Protective Marking 'UNOFFICIAL' may be assigned to information that Defence personnel and persons engaged under a contract have generated in their private capacity under reasonable use of Defence resource provisions.

Example: *Thomas sends an 'UNOFFICIAL' email to his co-workers inviting them to an after-work gathering to celebrate his birthday.*

Allison sends an 'UNOFFICIAL' email to her partner asking them to pick up milk on the way home from work.

Official Information

23. Official Information that is not sensitive and has a BIL rating of Low (1) should have the following Protective Marking:

a. 'OFFICIAL'.

Security Classified Information

24. Official Information that is determined to be sensitive and has a BIL rating of Low-Medium (2), High (3), Extreme (4) or Catastrophic (5) is classified information and should have a Security Classification as a Protective Marking.

25. Security Classifications are:

a. 'OFFICIAL: Sensitive';

b. 'PROTECTED';

c. 'SECRET'; and

d. 'TOP SECRET'.

26. A document may contain information covered by more than one Protective Marking. Where this occurs, the compilation of Official Information is to be assessed

against the criteria above and the appropriate classification assigned to the document. This Protective Marking is to be at least as high as the most sensitive or classified information or paragraph within the document.

Information Management Markers (IMMs)

27. An IMM is assigned to information where disclosure may be limited or prohibited by legislation, or where the information may otherwise require special handling. IMMs include:

a. legislative secrecy – for information that is subject to one or more legislative secrecy provisions;

b. personal privacy – for information that is personal information as defined in the *Privacy Act 1998*; and

c. legal privilege – for information that is subject to legal professional privilege.

Security Caveats

28. Security Caveats are additional Protective Markings applied to Official Information to advise of special protections that are to be applied to the information in addition to the security classification.

29. Some security caveats used in Defence are:

a. special handling instructions;

b. releasability caveats; and

c. Codewords.

30. **Special handling instructions**, including 'CABINET' and 'Exclusive for…' are caveats that are applied to Official Information requiring specific precautions.

a. '**CABINET**'. Cabinet documents are defined in the Cabinet Handbook and the *Freedom of Information Act 1982*. Official Information that includes Cabinet material, as defined in the Cabinet Handbook, **must** be marked with the 'CABINET' caveat and be classified 'PROTECTED' or higher.

b. '**Exclusive for …**' Indicates the information **must** be accessed only by the named recipient, and permission **must** be sought from the Originator before granting access to any other persons. This special handling instruction can only be used on Official Information classified 'PROTECTED' or higher.

31. 'CABINET' **must** be treated as accountable material. Further information on the storage, processing and transmission of documents with this special handling instruction can be found in the Australian Government Security Caveat Guidelines.

32. **Releasability Indicators**, including 'Australian Eyes Only' ('AUSTEO') and 'Australian Government Access Only' ('AGAO'), are caveats which permit or limit the release of Official Information to individuals based on citizenship or position.

33. The Defence Protected Network (DPN) is not accredited to store, process or communicate information bearing releasability indicators. In order to ensure that Defence remains compliant with various requirements of the Information Security Manual (ISM) and the PSPF, information bearing these caveats is not to be produced or stored on the DPN.

34. **'Releasable to …' ('Rel …').** The 'Rel …' caveat identifies Official Information with access limited to citizens of those countries listed in the Protective Marking. Access to 'Rel …' caveated information **must** be limited to citizens of the relevant countries and protected in accordance with the corresponding Security of Information Agreement or Arrangement or a General Security Agreement.

DSPF Control 15.1 – *Foreign Release of Official Information* provides the foreign release process and more information about the use of the 'Rel …' caveat under a Security of Information Agreement or Arrangement or a General Security Agreement.

Note: *All Defence-originated information is to be treated as approved by the originator for release to FVEY governments, unless subject to another releasability caveat.*

35. **'Australian Government Access Only' ('AGAO').** Access to 'AGAO' caveated information **must** only be released to people who are either:

a. Australian Government, Defence personnel or persons engaged under a contract who are Australian citizens;

b. United States, United Kingdom, Canadian or New Zealand Government officials on exchange, secondment, long-term posting or attachment, embedded as representatives of the Australian Government, whether located in Australia or Overseas, and who hold a current equivalent level security clearance issued by their government; or

Example: *A US citizen who is seconded by the US government to work in an Australian project office located in the US is eligible for AGAO access. This information is handled in the officers' capacity as an Australian Government representative and is not to be distributed to the officers' parent agency or government.*

c. United States, United Kingdom, Canadian or New Zealand citizens who have been granted an Australian security clearance on the basis of a citizenship eligibility waiver.

Example: *A foreign person engaged under a contract (not a FVEY government official) with a recognised US issued clearance working in an Australian Project Office is not eligible for 'AGAO' access and would require an Australian clearance issued on the basis of a citizenship eligibility waiver in order to access 'AGAO' caveated information.*

***Note**: Limitations apply to the extent of information access that can be granted under a citizenship eligibility waiver. See DSPF Principle 40 - Personnel Security Clearance for further information on these restrictions.*

36. Information with the 'AGAO' caveat **must not** be released to a foreign government, foreign company or any foreign entity, including foreign persons engaged under a contract with a foreign security clearance outside of the circumstances highlighted in paragraph 34.

37. 'AGAO' caveated information is not to be made accessible to United States, United Kingdom, Canadian or New Zealand nationals accessing Defence networks from coalition gateways. In this circumstance, these individuals are working on behalf of their own government and are not entitled to access 'AGAO' caveated information.

38. With the exception of those covered by exchange arrangements within the Defence intelligence agencies, foreign nationals granted approval to access 'AGAO' caveated information are required to sign a Certificate of Assurance for Access to Australian Government Access Only (AGAO) information by United States, United Kingdom, Canadian or New Zealand nationals. This Certificate is to be retained by the Security Officer or relevant business area.

39. **'Australian Eyes Only' ('AUSTEO').** The use of the 'AUSTEO' caveat is to be strictly limited and **must** only be released to Australian citizens.
A person who has dual Australian citizenship may be given AUSTEO caveated information, however, under no circumstances may the Australian citizenship requirement be waived.

***Note 1:** Australian citizens who hold dual citizenship with another country and have been granted an Australian clearance have had their allegiance and loyalty to Australia assessed during the security clearance process. They are therefore eligible to access 'AUSTEO' caveated information.*

***Note 2**: If the information is releasable to FVEY embedded officers, the 'AGAO' caveat should be applied.*

Legacy Protective Markings

40. For Official Information bearing legacy Protective Markings, please refer to Annex G for the appropriate equivalent marking and action.

41. **Special Access Program**. Additional requirements that apply to the handling of information relating to the Defence Special Access Program are in the Special Access Program Manual (available on the DSN).

42. There are specific limitations on the production and storage of information bearing security caveats on ICT systems. System users **must** only create, process or store information on systems which have been accredited to process such caveats.

Altering Protective Markings

43. Protective Markings **must not** be remarked (i.e. downgraded, removed or modified) without the written permission of the Originator of the information. Any modification of a Protective Marking without the Originator's authority is to be reported as a security incident in accordance with DSPF Principle 77 - *Security Incidents and Investigations*.

Exclusion: *Where the Originator has included declassification instructions within a document further permission to remark the document is not required provided the instructions are met.*

Exclusion: *Remarking of documents from former markings to their revised PSPF equivalents does not require the permission of the Originator. Refer to Annex I of this DSPF Control. However any caveats such as CODEWORD or release markings cannot be modified under these provisions and require Originator approval.*

44. Further information for reviewing and altering classifications is provided at Annex H of this DSPF Control.

Transfer/Transmission of Official Information

45. **Physical transfer of Official Information.** Requirements for the removal and physical transfer of classified information are provided in detail in DSPF Principle 71 - *Physical Transfer of Information and Assets*.

46. **Electronic transmission of Official Information.** Requirements for the electronic transmission of classified information are provided in the ISM and DSPF Principle 25 – *Information and Technology Security (Gateways and Data Transfer)*.

Appropriate Storage and Archive Requirements

47. **Physical access and storage.** Requirements for the physical access and storage of Official Information and assets are provided in DSPF Principle 72 - *Physical Security*.

48. **Registration.** Requirements for the registration of Official Information held by Defence are provided in Annex C of this DSPF Control.

49. **Filing.** Requirements for the filing of Official Information are provided in Annex F of this DSPF part, the *Archives Act 1983*, and the Defence Records Management Policy.

50. **Loss.** Any loss of Official Information is a security incident. The requirements for reporting and investigating security incidents are provided in DSPF Principle 77 - *Security Incidents and Investigations*.

Note: *Early reporting in accordance with DSPF Principle 77 - Security Incidents and Investigations may prevent further compromise and minimise the extent of damage of the security incident.*

51. **Copying and reproduction.** Requirements for the copying or reproduction of Official Information are provided in Annex I of this DSPF Control.

52. **Aggregated information.** Certain compilations of information 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 Business Impact Levels for further information.

ASD Compartment Information Storage and Handling Requirements

53. Defence personnel and persons engaged under a contract are to receive permission from the Originator if ASD-managed compartmented information needs to be held outside the Originator's facility or an accredited Sensitive Compartment Information Facility (SCIF).

54. Any permission from the Originator to file the documents in a specific location is to be recorded by the security officer in the area's security register. If granted, the ASD Records Management area is to be contacted to request a Special Series File. ASD is responsible for all Defence records management functions for Special Series Files or Sensitive Compartment Information (SCI) Records including file requests, musters, sentencing, storage, and disposal.

55. All SCI material is to be stored in the Special Series File managed by ASD. The information is not to:

a. be stored or processed on the DPN (including Objective);

b. be stored or processed on the Defence Secret Network (DSN; including Objective);

c. be held in any department corporate File other than a Special Series File; or

d. be transferred to central registries or to the national archives.

56. When no longer required, all Special Series Files are to be returned to ASD.

57. Special provisions for the custody of intelligence information are made in the *Archives Act 1983* Section 29(8). Further information can be found in the Defence Records Management Policy.

Protecting Foreign Information

58. Defence personnel and persons engaged under a contract **must** handle foreign government information with a level of protection no less stringent than that provided by the Originator.

59. In many cases, the Australian government has provided an assurance to safeguard this information under the terms of a Security of Information Agreement or Arrangement (SIA) or a General Security Agreement (GSA). For example, foreign government information **must** be compartmentalised to ensure it is protect from unauthorised third party access.

60. Defence personnel and persons engaged under a contract **must** protect foreign government information in accordance with all relevant SIAs and GSAs. A complete list of Defence's SIAs is available on the Defence Security site on the Defence Secret Network (DSN).

Note: *A list of SIAs at the OFFICIAL level is available on the DPN.*

61. For more information on SIAs and GSAs, contact 1800DEFENCE.

62. In addition, Project Security Instructions (PSI) may apply to project-specific foreign information. Defence personnel and persons engaged under a contract are to protect foreign information in accordance with all relevant PSI as long as they do not contradict the relevant SIA or GSA.

Key Definitions

63. **Accountable material.** Accountable material is information that requires the strictest control over its access and movement including TOP SECRET security classified information and some types of caveated information such as 'CABINET'.

64. **Classification Process.** The process by which the confidentiality requirements of Official information are assessed and the appropriate Protective Markings applied.

65. **Commonwealth Record.** Defined by the *Archives Act 1983* as a Record that:

a. is the property of the Commonwealth or a Commonwealth institution; or

b. is deemed to be a Commonwealth record by virtue of the *Archives Act 1983*, but does not include a Record that is exempt material or is a register or guide maintained in accordance with Part VIII of the *Archives Act 1983*.

66. **File.** Either:

a. an organised unit of documents, accumulated during current use and kept together because they deal with the same subject, activity or transaction; or

b. in electronic archives and records, two or more data records dealing with the same subject, activity or transaction that are treated as a unit.

67. **Information Management Marker (IMM).** A way to identify information that has non-security related restrictions on access and use due to legal, legislative or privacy sensitivities. Information Management Markers are not Protective Markings. IMMs used in Defence are:

a. 'Personal Privacy';

b. 'Legal Privilege'; and

c. 'Legislative Secrecy'.

68. **National Interest.** A matter which has or could have an impact on Australia, including:

a. national security;

b. international relations;

c. law and governance, including:

(1) interstate/territory relations;

(2) law enforcement operations where compromise could hamper or prevent national crime prevention strategies or endanger personal safety;

d. economic wellbeing; and

e. heritage or culture.

69. **National Security Information.** National Security Information is any official resource (including assets) that records information about or is associated with Australia's:

a. protection from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system, acts of foreign interference and the protection of Australia's territorial and border integrity from serious threats; or

b. defence capability.

70. **Official Information.** Any information received, developed or collected by, or on behalf of, the Australian Government, through its agencies and persons engaged under a contract that includes:

a. documents and paper;

b. data;

c. software or systems and networks on which the information is stored,

d. intellectual information (knowledge) acquired by individuals; and

e. physical items from which information regarding design, components or use could be derived.

71. **Originator.** The entity that created the Official Information or on whose behalf the Official Information was created. An Originator can be:

a. a military or business unit within Defence;

b. an Australian government department or agency;

c. a foreign government; or

d. a person who has been authorised and has received appropriate training to conduct declassification of intelligence information within specified intelligence compartments on behalf of the intelligence compartment controller.

72. **Protective Marking.** A marking given to Unofficial and Official Information to indicate the level of protective measures that are to be applied during use, storage, transmission, transfer and disposal so as to reduce the risk of unauthorised disclosure. Protective Markings used in Defence are:

a. 'UNOFFICIAL';

b. 'OFFICIAL';

c. 'OFFICIAL: Sensitive';

d. 'PROTECTED';

e. 'SECRET'; and

f. 'TOP SECRET'.

73. **Public Release.** Unlimited public access or circulation of Official Information, for example by way of Defence publications or websites. The need-to-know principle does not apply once the information enters the public domain.

74. **Record.** Defined by the *Archives Act 1983* as a document, or an object, in any form (including any electronic form) that is, or has been, kept by reason of:

a. any information or matter that it contains or that can be obtained from it; or

b. its connection with any event, person, circumstance or thing.

75. **Security Caveat.** Applied to security classified information indicating that special protective requirements apply in addition to those associated with its Security Classification. Security Caveats used in Defence include:

a. Special handling instructions:

(1) 'CABINET'; and

(2) 'Exclusive for …'.

b. Releasabillity indicators:

(1) 'Australian Eyes Only' ('AUSTEO');

(2) 'Australian Government Access Only' ('AGAO'); and

(3) 'Releasable to…' ('Rel …').

76. **Security Classification.** A type of Protective Marking assigned to security classified information that indicates the consequence of unauthorised disclosure and convey to users the level of protection needed during use, storage, transmission, transfer and disposal. Security Classifications used in Defence are:

a. 'OFFICIAL: Sensitive';

b. 'PROTECTED';

c. 'SECRET'; and

d. 'TOP SECRET'.

77. **Unofficial Information.** Non-work related information generated by Defence personnel and persons engaged under a contract under reasonable use of Defence resource provisions, typically contained in email, faxes etc.

Further Definitions

78. Definitions for common Defence administrative terms can be found in the Defence Instruction.

Annexes and Attachments

Annex A – *Selecting an Appropriate Protective Marking*

Annex B – *Applying Protective Markings 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*

Document administration

Identification

DSPF Control	Classification and Protection of Official Information
Control Owner	AS SPS
DSPF Number	10.1
Version	7
Publication date	28 April 2025
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 and Technology Security (Physical) Information and Technology Security (Personnel) 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.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy; restructure to present information of most use up front.
4	28 August 2020	AS SPS	Update of mandatory statements regarding the need-to-know principle, security clearances, and the AUSTEO caveat
5	26 March 2021	AS SPS	Introduction of 'NATIONAL CABINET' caveat. Amended 'CABINET' from sentence case to capital letters, in line with Caveat Guidelines.

Version	Date	Author	Description of changes
6	28 June 2024	AS SPS	Control Owner review; clarify terminology and definitions; specifically ‘REL..’, ‘AGAO’ and ‘AUSTEO’ caveats, update of OFFICIAL: Sensitive as security classified information.
7	28 April 2025	AS SPS	Removal of ‘NATIONAL CABINET’ caveat from document.

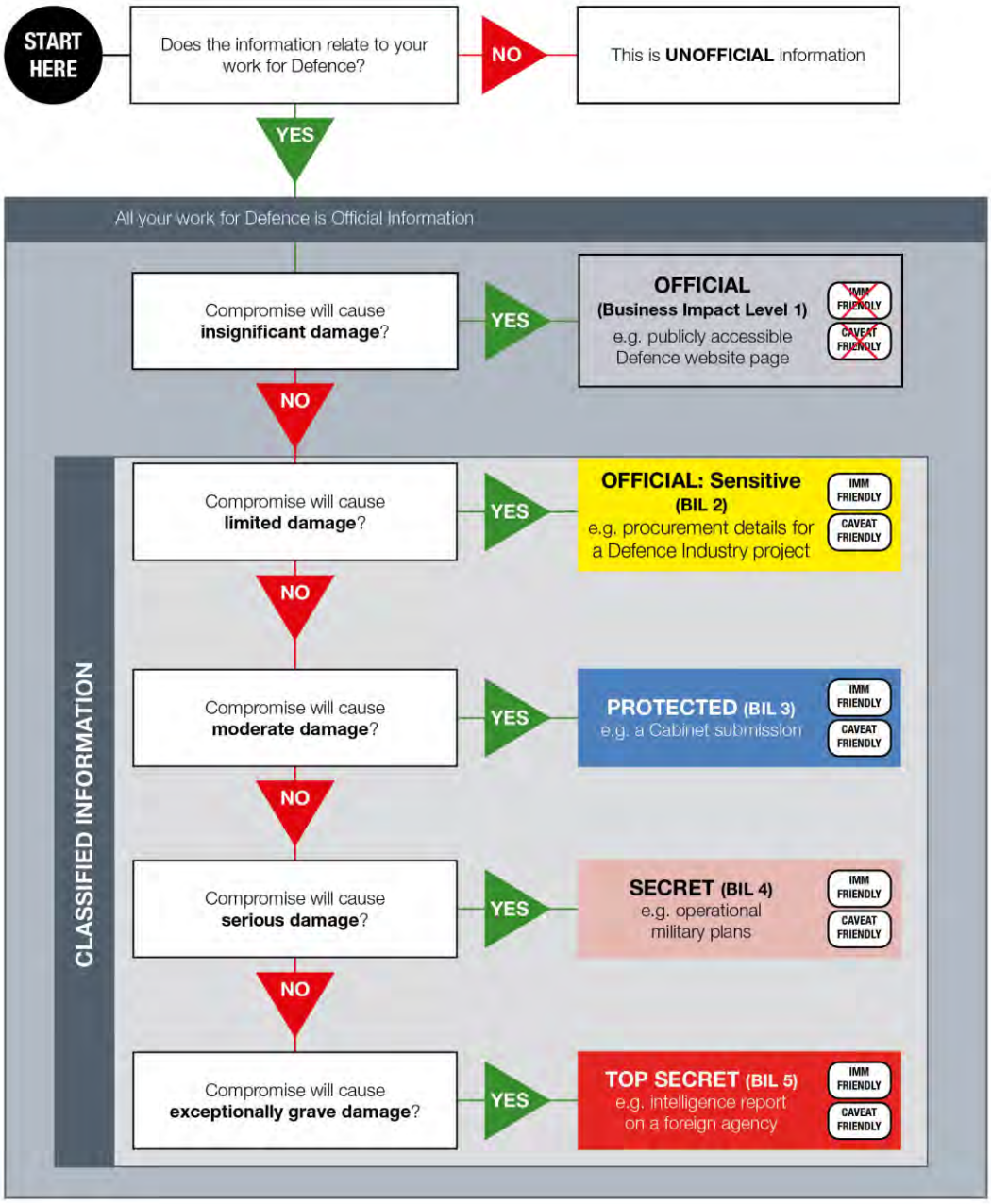
Australian Government
Defence

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.

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	4
Annex Publication date	28 June 2024
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.
3	31 July 2020	AS SPS	Protective Marking update of text and info-graphic to align with PSPF
4	28 June 2024	AS SPS	Update graphic to incorporate Business Impact Levels and link to Table 1 in Control 10.1

Australian Government
Defence

Defence Security Principles Framework (DSPF)

Annex B to Classification and Protection of Official Information– Applying Protective Markings 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 (eg. Font size 14, Arial Bold). 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 over-stamping be in red.

Applying Paragraph Markings

4. It is recommended that individual paragraphs of a document be protectively marked where multiple markings appear. 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 order of precedence or hierarchy for protective markings is:

a. classification; foreign government information markings (if any);

b. caveats or other special handling instructions (if any); then

c. Information Management Markers (IMM) (if any).

6. 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, Information Management Markers (IMM) and special handling caveats are abbreviated as follows:

a. ‘OFFICIAL’ – (O);

b. ‘OFFICIAL: Sensitive’ – (O:S);

c. ‘Legal privilege’ (Legal);

d. ‘Personal secrecy’ (Pers);

e. ‘Legislative secrecy’ (Leg);

f. ‘Cabinet’ (Cab);

g. ‘PROTECTED’ (P);

h. ‘SECRET’ (S); and

i. ‘TOP SECRET’ (TS).

7. A paragraph marking key is to be used on all paragraphs in a paragraph marked document.

8. Legacy Protective Markings For Official Information bearing legacy Protective Markings, please refer to Annex G for the appropriate equivalent marking and action.

Protectively Marking Document Titles

9. It is recommended, if possible, that the title of a document be marked no higher than ‘OFFICIAL’ to ensure ease of reference.

10. If the title needs to be classified, the relevant Protective Marking is to appear abbreviated in brackets after the last word of the title.

a. To enable reference to a document with a classified title, it is recommended the Originator apply an OFFICIAL abbreviated title or reference number and date.

Printed Graphic Material

11. 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.

Protectively Marking Annexes, Appendices and Covering Documents

12. Sometimes the annex or appendix to a document requires a different protective marking from the document itself. If the annex or appendix has a higher protective marking or 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: *'SECRET-covering-TOP SECRET'*

Example: *'OFFICIAL-covering-PROTECTED'*

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

Example: *'OFFICIAL-covering-SECRET'*

14. 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

15. Large compilations of Official 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

16. Photographs and film requiring protection and their storage envelopes or containers are to carry a conspicuous Protective Marking. Security classified imagery (including roll imagery, cine-film, video tape) requires further 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

17. Presentations containing Official Information are to bear Protective Markings. 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 Official Information and these are to be marked accordingly.

Audio

18. 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

19. 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

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

a. DSPF Principle 21 - *Information and Technology Security (Physical)*; and

b. the Information Security Manual (ISM).

21. 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	4
Annex Publication date	28 June 2024
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.
3	31July 2020	AS SPS	Protective Marking update to align with PSPF
4	28 June 2024	AS SPS	Control Owner review; clarify requirements

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 and persons engaged under a contract 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 a Protective Marking.

***Note**: The alteration of a protective marking means to change a protective marking's protection requirements. A change in a protective marking due to a change of Whole-of-Government classification guidelines (re-marking) is not in-scope for this definition. For information re-marking classified documents, see Annex I – Remarking Information Bearing Former Security Classifications*

4. 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 Defence Security (FAS DS) if an appropriate Group or Service cannot be identified as holding the functions and responsibilities of the original unit. FAS DS may delegate this authority if required.

***Note**: The Originator is the functional position from which the information was originally prepared, not the individual who prepared the document.*

5. For printed material (less than 15 years old), 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.

6. **Printed Material** (over 15 years old), the Protective Marking is to be changed by updating the metadata in the file management system. No changes can be made to the physical documents as these are considered archival records by the National Archives of Australia (NAA).

7. **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.

8. **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.

9. **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,

***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 record is altered. Changes to the information about the record, including the classification, must be recorded in the metadata.*

where a change will be made to its Protective Markings.

10. **Removal**. Removal of any information from a file is to be completed in accordance with Defence Records Management Policy. For further information, refer to the Defence Records Management Policy.

11. **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 Defence Records Management Policy for further information.

***Note**: The DCARR does not provide a general declassification service for Defence. However, 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.*

12. 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	4
Annex Publication date	28 June 2024
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 2018	AS SPS	Foundational review; PSPF update; and security classification alignment.
3	31 July 2020	AS SPS	Protective Marking update to align with

Version	Date	Author	Description of changes
			PSPF; update of language to reflect Defence Admin Policy
4	28 June 2024	AS SPS	Control Owner review; clarify requirements, specifically archive requirements

Defence Security Principles Framework (DSPF)

Annex D to **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 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 Official 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 and covered by a General Security Agreement (GSA) or Security of Information Agreement or Arrangement (SIA);

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 DSPF to protect the information.

Public Release

6. Public release of Official Information, including through a tender briefing, is to be done in accordance with the Defence Media and Communication Policy.

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. Information classified as 'OFFICIAL: Sensitive' or marked with an IMM **must** only be released to a person or organisation outside of Defence when an agreement or arrangement, such as a contract or deed, is in place which governs how the information is used and protected.

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. Official Information that is 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 under exceptional circumstances. Refer to DSPF Principle 41 - Temporary Access to Classified Information and Assets for release criteria that apply to access to 'PROTECTED' material without a BASELINE security clearance.*

State, Territory and Local Governments

12. The release of Official 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 Regional Office or relevant Executive Security Adviser.

Courts

13. 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 Defence Security about the release of the documents.

Parliamentary Committees

14. 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	4
Annex Publication date	28 June 2024
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 Annex	Release 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.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	28 June 2024	AS SPS	Control Owner review; clarify requirements

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.

2. All information classified 'SECRET' and above, and accountable material, held by Defence Industry Security Program (DISP) members **must** be registered. Information at other classifications held by DISP 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. 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 'OFFICIAL' reference title. With due care, the CDR should rarely need to be classified unless the aggregation of the information warrants it.*

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 Protected Network (DPN) 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 Defence Records Management Policy.

d. The preferred method of distributing documents is by sending an Objective link. When a document classified 'SECRET' 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	4
Annex Publication date	28 June 2024
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.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF
4	28 June 2024	AS SPS	Control Owner review; clarify requirements

Australian Government
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 Defence Records Management Policy.

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 Protective Markings. Refer to Annex G for further information on legacy classifications and equivalences.*

3. Official Information that can be filed is to be placed on an appropriate file as soon as possible after its creation or receipt.

File Types

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

a. 'TOP SECRET' – red;

b. 'SECRET' – salmon/pink;

c. 'PROTECTED' – blue (formerly: green plus stripe pre-01 October 2018 PSPF revision); and

d. 'OFFICIAL: Sensitive' – yellow.

Active File Types with outdated Protective Markings

5. Active files that carry former Protective Markings should be remarked with an updated equivalent Protective Marking. The following applies:

a. Former 'CONFIDENTIAL' – green (Files should be closed to new documents, active information in the file should be reassessed, marked and stored appropriately);

b. Former 'RESTRICTED' and 'X-in-Confidence' file covers may continue to be used, over stamp the former protective marking with the new protective marking and remark the file in the appropriate records management system.

Filing Procedures

6. 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.

7. 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.

8. 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

9. A file census of information classified 'PROTECTED', 'CONFIDENTIAL' (if active files remain), '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.

Note: *Spot checks for highly classified or caveated information (SECRET/TOP SECRET) are to be conducted regularly. Personnel can conduct spot checks by sighting documents listed in the register and documenting the process.*

How to Conduct a File Census:

10. 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.

11. 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*.

Note: *For further guidance on conducting a file census or audit, please refer to section C.5.2.3 of PSPF Policy 8 – Classification System.*

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Official Information Filing and File Census
Annex Version	4
Annex Publication date	28 June 2024
Releasable to	Defence and Defence Industry
Compliance	Compliance requirements for this supplementary document are the

DSPF Annex	Official Information Filing and File Census
Requirements	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.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF
4	28 June 2024	AS SPS	

Defence Security Principles Framework (DSPF)

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

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 E of this DSPF Control for further information on scanning documents into Objective.*

2. For information classified 'SECRET' and above, Defence Industry are to record details of copies and reproductions in a Form AC458 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 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	3
Annex Publication date	31 July 2020
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.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF

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 Defence Records Management Policy.*

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 information registered 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.

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 Originator.

5. A CDR is to be maintained as long as any one document recorded is still in existence. 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 the Defence Records Management Policy.

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

7. **Caveat – CABINET (Previously DLM Sensitive: Cabinet)** Information which bears the CABINET caveat 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 Principle 13 – *Communications Security* 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.*

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. Official 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 person/s engaged under a contract. 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 person/s engaged under a contract 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	5
Annex Publication date	28 June 2024
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.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	29 September 2020	AS SPS	Update of Cabinet Handbook hyperlink
5	28 June 2024	AS SPS	Control Owner review; clarify language

Defence Security Principles Framework (DSPF)

Annex I to Classification and Protection of Official Information – Remarking Information Bearing Former Protective Markings

1. The Attorney-General's Department updated the Protective Security Policy Framework (PSPF) in October 2018, and included a revised system of Protective Markings for classified information and assets. All non-corporate Commonwealth Agencies were required to transition to the revised system by 01 October 2020.

Legacy Protective Markings

2. There are legacy Protective Markings in circulation across the Australian Government that no longer reflect Government or Defence security policy. Defence personnel and persons engaged under a contract are required to handle, transfer, transmit and store Official Information with a legacy Protective Marker in accordance with their current equivalency as detailed in Table 1 of this Annex.

3. Protective Markers on published documents do not require marking, but should be handled in accordance with their current equivalent as detailed in Table 1.

4. Existing documents that are still in use and all new documents require marking in accordance with the Protective Markers detailed in this Control.

5. The remarking of documents from legacy Protective Markers to the current Protective Markers does not require the permission of the Originator. However, any caveats such as CODEWORD or release markings cannot be modified under these provisions and require Originator approval.

Table 1: Legacy Protective Markings and their current equivalency

Legacy Protective Marking	Date Ceased in Defence	Current Equivalent
'UNCLASSIFIED'	22 June 2020	'OFFICIAL'
'For Official Use Only'	22 June 2020	'OFFICIAL: Sensitive'
'CONFIDENTIAL'	22 June 2020	Discontinued; Follow requirements for 'SECRET'.
'Sensitive'	22 June 2020	'OFFICIAL: Sensitive' *There is no direct equivalent under the new Information Management Markers.
'Sensitive: Cabinet'	22 June 2020	'PROTECTED' or higher *'Cabinet' is now a caveat with specific handling instructions. It can only be used with a security classification.
'Sensitive: Personal'	22 June 2020	'Personal privacy' *Must be used with the Protective Marker of 'OFFICIAL: Sensitive' or higher.
'Sensitive: Legal'	22 June 2020	'Legal privilege' *Must be used with the Protective Marker of 'OFFICIAL: Sensitive' or higher.
'HIGHLY PROTECTED'	01 August 2012	'SECRET'
'RESTRICTED'	01 August 2012	'OFFICIAL: Sensitive'
'LEGAL-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Legal privilege'.
'CABINET-IN-CONFIDENCE'	01 August 2012	'PROTECTED' or higher with the caveat 'Cabinet'.
'COMMERCIAL-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive'
'AUDIT-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy' if it includes personal information.

Legacy Protective Marking	Date Ceased in Defence	Current Equivalent
'SECURITY-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy' if it includes personal information.
'COMMITTEE-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive'
'MEDICAL-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy'.
'PSYCHOLOGY-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy'.
'CLIENT-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy'.
'STAFF-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy'.
'HONOURS-IN-CONFIDENCE'	01 August 2012	'OFFICIAL: Sensitive' with the IMM 'Personal privacy'.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Remarking Information Bearing Former Security Classifications
Annex Version	4
Annex Publication date	28 June 2024
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.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy Updated Protective Markings.
4	28 June 2024	AS SPS	Control Owner review; clarify requirements

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Security for Projects

General principle

1. Projects of a type referred to in the Expected Outcomes below, with an appropriate Steering Group (SG), need to incorporate security planning into project activities and all stages of the One Defence Capability System. 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 SGs 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 One Defence Capability System.

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.

7. Project Security Risk is considered and managed through this Principle and Defence Security Principles Framework (DSPF) Control 11.1 – Security for Projects, alongside other risk under Accountable Authority Instruction 1 - Managing Risk and Accountability. DSPF 4a, Governance and Executive Guidance also provides framing for Defence Security Risk management.

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 Functions Delivery (ASFD) through Branch Head (or equivalent)
High	Defence Security Committee (DSC) – through ASFD
Extreme	DSC – through ASFD

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

Consideration may also be given to brief the Project Managers chain of command prior to elevating risks to ASFD.

Document administration

Identification

DSPF Principle	Security for Projects
Principle Owner	First Assistant Secretary Defence Security Division (FAS DS Division)
DSPF Number	Principle 11
Version	3
Publication date	1 September 2023
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 11.1
Control Owner	Assistant Secretary Functions Delivery (ASFD)

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) **Standards**: AS: 4811-2006: Employment screening
Read in conjunction with	Defence Security Principles Framework 4a, Governance and Executive Guidance **Principles:** 12 - Security for Capability Planning; 16 – Defence Industry Security; and 82 – Procurement. Capability Program Management Manual
See also DSPF Principle(s)	**Principles:** 10 – Classification and Protection of Official Information; 15 – Foreign Release of Official Information; 17 – Information Systems (Physical) Security; 18 – Information Systems (Personnel) Security; 19 – Information Systems (Logical) Security; 23 – ICT Certification and Accreditation 40 – Personnel Security Clearance; 41 – Temporary Access; and 71 – Physical Transfer of Official Information, Security Protected and Classified Assets.
Implementation Notes, Resources and Tools	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 or your Executive Security Adviser (ESA). 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
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	1 September 2023	FAS DS	Amendments to update with the release of the Capability Program Management Manual, the One Defence Capability System, and administrative changes.

Defence Security Principles Framework (DSPF)

Security for Projects

Control Owner

1. The Assistant Secretary Functions Delivery (ASFD) 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 Defence Security Division (FAS DS Division) is the Policy Owner for security.

2. The ASFD is also the Policy Owner for Program Management under the Acquisition & Sustainment domain. The Deputy Secretary, Capability Acquisition & Sustainment Group (DEPSEC CASG) is the relevant Accountable Officer. The Executive Director Program Management is the Program Management Function Lead as defined in the Capability Acquisition and Sustainment Group Business Framework.

Framework Escalation Thresholds

3. Security Risk Responsibility allocation does not override overall Risk Management Responsibilities as articulated in Accountable Authority Instruction 1 - Managing Risk and Accountability.

4. The ASFD has set the following general threshold for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

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 Functions Delivery (ASFD) through Branch Head (or equivalent)
High	Defence Security Committee (DSC) – through ASFD
Extreme	DSC – through ASFD

Note: *Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel. Refer Annex A within for flow chart.*

Consideration may also be given to brief the Project Managers chain of command prior to elevating risks to ASFD.

Controls

Project Security Planning

5. On appointment of an appropriate Steering Group (SG) under the One Defence Capability System, 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.

6. 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.

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

Project Security Function

8. Projects are to consider the need for the appointment of a Project Security Officer.

9. In addition to a Project Security Officer, an appropriate SG 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.

10. The composition of SG members will depend on the Project. Membership may comprise representation from:

a. the Project Owner / Project Sponsor;

b. the Executive Security Advisor (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 Service Delivery Division, Security and Estate 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.

11. The Project security function should advise the SG 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

12. Project security costs are to be identified and resourced throughout all stages of the planning for and execution of a Project (refer to Pages - Project Controls). Security costs are to be identified for all Fundamental Inputs to Capability (FIC) throughout all stages of the One Defence Capability System. 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:

(1) gaining facility or ICT system accreditation; and

(2) 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:

(1) in service security costs such as additional security clearances, physical security infrastructure and enhanced guarding requirements on introduction to service; and

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

Project Security Reviews

13. 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.

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

a. Decision making forums convened by appropriate 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.

15. 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:

(1) confirm compliance with security policy;

(2) ensure adequate risk mitigation strategies are in place; and

(3) 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 One Defence Capability System Phase

Strategy and Concepts Phase

16. 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.

17. 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.*

18. 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 Division (DS Division) 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 on the Defence Security Portal; 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. DS Division 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 Project.Security@defence.gov.au at the earliest possible stage of the project*

*The PID, PSI and SCCG may not be mature at this Phase of the One Defence Capability System. They **must**, however be reviewed and updated in line with each Integrated Project Management Plan update and each Gate Review.*

19. 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.

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

21. 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.

22. 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.

23. Research projects, and projects other than capital and intelligence projects, are not required to submit any of the above documentation to DS Division; 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:

(1) a development unique to Australia that might have marketing potential;

(2) individuals or organisations outside of Defence, such as academic or commercial research and development specialists; and

(3) a patent application.

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

Risk Mitigation and Requirements Setting Phase

25. 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:

(1) solution specific risks, including Capability risks and any shared risks introduced by a proposed solution; and

(2) associated security costs.

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

27. 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.

28. If changes are made during negotiations, the PID should be resubmitted to the DS Division before contract signature.

Note: *The PID, PSI and SCCG* ***must*** *be reviewed and updated in line with each Integrated Project Management Plan update and each Gate Review, and forwarded to DS Div at project.security@defence.gov.au.*

Acquisition Phase

29. 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.

30. 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.

Note: *The PID, PSI and SCCG* ***must*** *be reviewed and updated in line with each Integrated Project Management Plan update and each Gate Review, and forwarded to DS Div at project.security@defence.gov.au.*

In-Service and Disposal Phase

31. 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.

32. 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.

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

34. During project closure, Integrated Project Managers should:

a. review the project's security performance and provide a report to the DS Division, 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.

Note: *The PID, PSI and SCCG* ***must*** be reviewed and updated in line with each Integrated Project Management Plan update and each Gate Review*, and forwarded to DS Div at project.security@defence.gov.au.*

Roles and Responsibilities

First Assistant Secretary Defence Security Division

35. FAS DS Division is responsible for:

a. providing protective security advice to Integrated Project Managers and Project 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

36. Capability Managers, 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

37. 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

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

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

39. The Program Sponsor is accountable to the Capability Manager for:

a. the management of security within the Project, including setting and controlling the project security tolerances and reporting requirements; and

b. ensuring that the outcomes of all program activities are achieved and aligned with Defence strategic objectives.

Program Manager

40. 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

41. The Project Sponsor is accountable to the Capability Manager through the Program Sponsor for the management of security within the Project and is to work in partnership with the Integrated Project Manager to ensure capability outcomes are delivered.

Integrated Project Manager

42. 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 Division of the nature of larger projects and anticipated security impacts to facilitate the provision of advice to Project Managers and Project Security Officers by DS Division;

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 Project 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 - *Cyber Security Assessment and Authorisation* and DSPF Principle 73 – *Physical Security Certification and Accreditation*;

g. ensuring that appropriate security classification guidance is available to all Defence personnel and persons engaged under a contract 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.

Project Security Officer

43. Project 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 - *Cyber Security Assessment and Authorisation* 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*.)

44. For small Project teams, the Integrated Project Manager may fulfil the role of Project Security Officer.

Defence Special Access Programs Project Managers

45. 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. The Special Access Programs Manual assigns responsibilities and prescribes security procedures for implementation and use in the management, administration and oversight of all Defence SAPs.

Key Definitions

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

47. **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 One Defence Capability System (ODCS) process.*

48. **Steering Group**. The organisational entity established within the primary delivery and enabler Group which performs Project functions as part of the One Defence Capability System process. It is comprised of representatives from all relevant stakeholders, and may be an Integrated Project Management Team.

49. **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.

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

51. **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 One Defence Capability System.

52. **Resident project teams**. Defence personnel and/or persons engaged under a contract based overseas with foreign prime contractors on Defence acquisition Projects.

53. **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.

54. **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.

55. **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.

56. **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.

57. **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, 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

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

Annexes and Attachments

Annex A: Project Security Risk Escalation Thresholds Flow Chart

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

Document administration

Identification

DSPF Control	Security for Projects
Control Owner	Assistant Secretary Functions Delivery (AS FD)
DSPF Number	Control 11.1
Version	3
Publication date	1 September 2023
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 10 – Classification and Protection of Official Information; 12 – Security for Capability Planning; 15 – Foreign Release of Official Information; 16 – Defence Industry Security Program 17 – Information Systems (Physical) Security; 18 – Information Systems (Personnel) Security; 19 – Information Systems (Logical) Security; 23 – ICT Certification and Accreditation 40 – Personnel Security Clearance; 41 – Temporary Access; 71 – Physical Transfer of Official Information, Security Protected and Classified Assets; and 82 – Procurement.

Version control

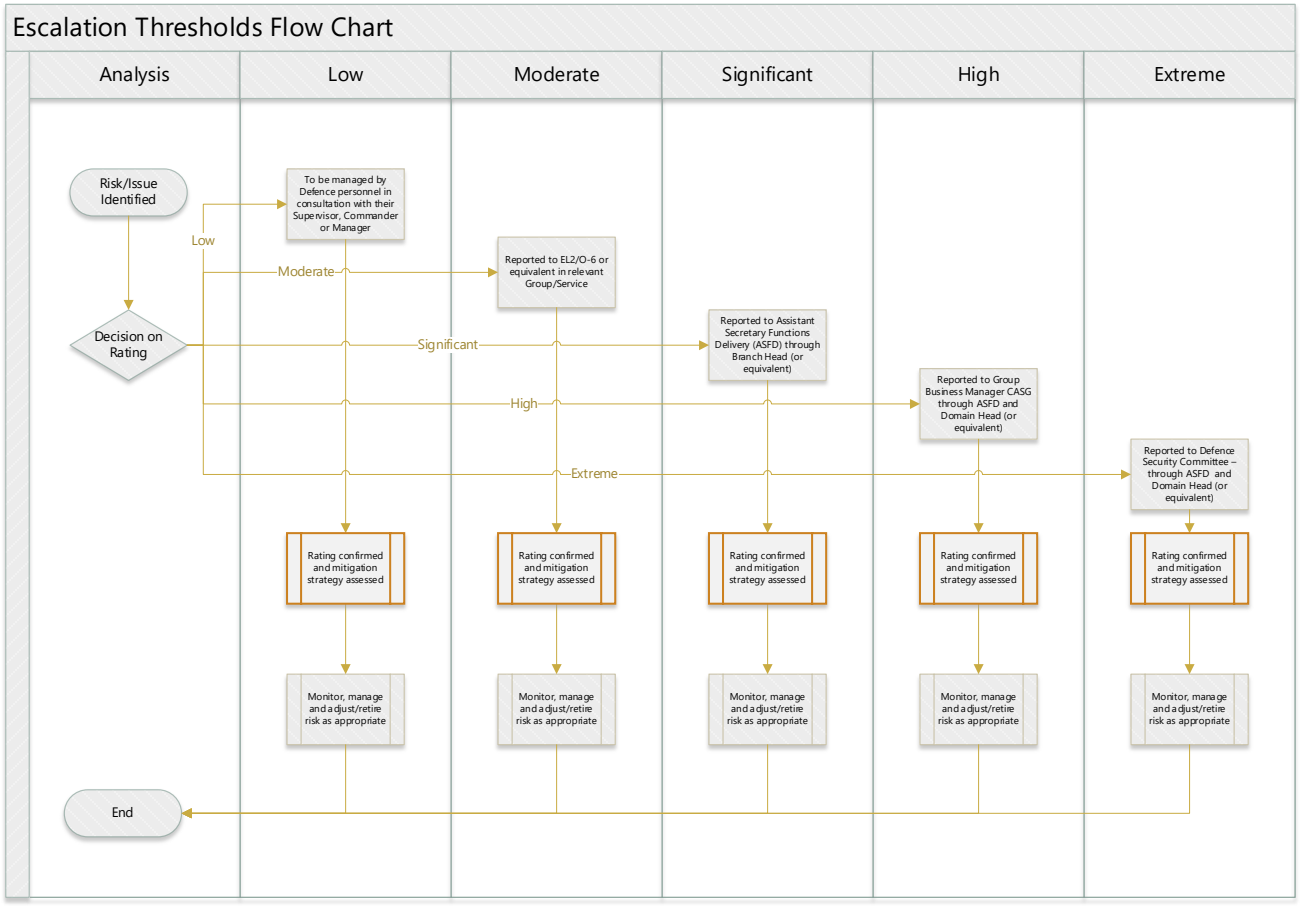
Note: A new row is added for each version to show the version history of this document.

Version	Date	Author	Description of changes
1	2 July 2018	AS PM	Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	1 September 2023	AS FD	Amendments to update with the release of the Capability Program Management Manual, the One Defence Capability System the CASG Control Owner and administrative changes.

Australian Government
Defence

Defence Security Principles Framework (DSPF)

Annex A to Security for Projects – Project Risk Escalation Thresholds Flow Chart



Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Project Risk Escalation Thresholds Flow Chart
Annex Version	1
Annex Publication date	01 September 2023
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 for Projects
DSPF Number	Control 11.1

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	01 September 2023	AS FD	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: *Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel.*

Document administration

Identification

DSPF Principle	Security for Capability Planning
Principle Owner	First Assistant Secretary Security and Vetting Service
DSPF Number	Principle 12
Version	2
Publication date	31 June 2020
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	ASIO, Security Equipment Guides (SEGs) are available from theGovDex 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
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy

Defence Security Principles Framework (DSPF)

Foreign Release of Official Information

General principle

1. The release of Official 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 Official Information marked with a Dissemination Limiting Marker and/or an Information Management Marker:

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

7. Foreign Release of classified Official 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 Official Information outside of a GSA/SIA:

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

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

Document administration

Identification

DSPF Principle	Foreign Release of Official Information
Principle Owner	First Assistant Secretary Security & Vetting Service (FAS S&VS)
DSPF Number	Principle 15
Version	3
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 15.1
Control Owner	Assistant Secretary Security Policy and Services

Related information

Legislation	Criminal Code Act 1995
Government Compliance	**PSPF 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)	Assessing and Protecting Official Information
Implementation Notes, Resources and Tools	PSPF Annual Release General Security Agreements (GSA)/Security of Information Agreements/Arrangements (SIA) for the reciprocal 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	02 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.
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy

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 Enterprise-wide Control.

Escalation Thresholds

2. The escalation thresholds outlined below apply in circumstances where a stakeholder cannot follow, or deviates from, the mandated process in this Control.

	Responsibility	
Risk Rating	**Classified Information being shared under a Security of Information Agreement or Arrangement (SIA)/ General Security Agreement (GSA)**	**Classified Information being shared outside of an SIA/GSA**
Low	EL1/O5 or equivalent in relevant Group/Service	Director Strategic and International Security Policy
Moderate	EL2/O6 or equivalent in relevant Group/Service	AS SPS
Significant	Assistant Secretary Security Policy and Services (AS SPS)	AS SPS
High	AS SPS	FAS DS
Extreme	First Assistant Secretary Defence Security (FAS DS)	FAS DS

Note: Persons engaged under a contract are not authorised to depart from Defence Administrative Policy without approval from appropriate Defence personnel. Delegations and decision making authorities are position based (e.g. FAS DS).

Introduction

3. This DSPF Control provides guidance on releasing Official Information to Foreign Entities in a manner that balances the benefits of sharing information against the likelihood and consequences of harm.

a. All information received, developed or collected by, or on behalf of, the Australian Government by Defence personnel and persons engaged under a contract in their professional capacity is considered “Official”.

4. The foreign release process ensures Defence meets its legal and policy obligations when sharing Official Information with Foreign Entities. This process applies both when Foreign Entities are overseas or in Australia.

5. Additional guidance on the foreign release process, and visual tools, can be found in the Annexes of this DSPF Control.

Security of Information Agreements/Arrangements and General Security Agreements

6. The Australian Government can enter into a Defence-specific Security of Information Agreement or Arrangement (SIA) or a Whole-of-Government General Security Agreement (GSA) with another Foreign Entity that specifies the conditions under which Official Information can be exchanged.

7. These instruments establish protective standards and security classification equivalencies. Where 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 to a standard that is no less stringent than that of the releasing party.

8. The existence of an SIA/GSA does not automatically allow the release of classified information, but provides a measure of assurance from a foreign government that Official Information released to Foreign Entities will be appropriately protected.

a. A list of Defence’s and Australia’s SIAs/GSAs is available here. If you are unsure if an SIA/GSA exists for a particular country, please contact Defence Security Division via dsp.international@defence.gov.au.

b. An SIA/GSA may only be used for the actions or activities outlined in the relevant agreement or arrangement. For example, if the SIA/GSA only covers the exchange of Defence-originated information, it cannot be used by non-Defence organisations.

c. An SIA/GSA may only be used to share classified information between the parties identified by the SIA/GSA itself. For example:

(1) The AUS-NATO SIA is only applicable in instances where information is being released in support of NATO. As a result, the AUS-NATO SIA cannot be used to share AUS information directly with a NATO member state. This would require a specific bilateral SIA/GSA with that member state.

Principles of Foreign Release

9. The release of Official Information is built on five elements:

(1) whether or not an SIA/GSA exists;

(2) the recipient having a need-to-know;

(3) written approval from the Originator (for classified information);

(4) if necessary, the recipient having a recognised security clearance when information is released under an SIA/GSA; and

(5) if necessary, approval from a Foreign Release Authority.

Treatment of Official Information by marking

OFFICIAL information

10. Information with the protective marking OFFICIAL may be released to Foreign Entities on a need-to-know basis and does not require approval by a Foreign Release Authority.

Security Classified Information – OFFICIAL: Sensitive Information

11. OFFICIAL: Sensitive information shared under an SIA/GSA may be released to Foreign Entities on a need-to-know basis, providing Originator approval is granted. Release of OFFICIAL: Sensitive information shared under an SIA/GSA does not require approval by a Foreign Release Authority.

12. A Foreign Release Authority **must** approve the release of OFFICIAL: Sensitive information outside of an SIA/GSA.

Security Classified Information – PROTECTED and above information

13. All security classified information with the security classification PROTECTED or above may be released to Foreign Entities on a need-to-know

basis, providing Originator approval is granted. This release **must** be approved by a Foreign Release Authority.

Note: *Refer to* ***Table 1: Foreign Release Authority*** *to determine the minimum level of Foreign Release Authority approval required. The level of approval required will depend on the security classification of the information and whether an SIA/GSA is extant. At their discretion, Groups and Services may escalate responsibility to a level higher than outlined in the table.*

Foreign Release Authority

14. A Foreign Release Authority **must** be an APS or ADF official at the specified level/rank in the Requester's chain of command, who can make an informed decision about whether to approve or deny a foreign release request.

a. The Foreign Release Authority may choose to escalate this authority to a higher level/rank within their chain.

15. Defence Security Division acts as the final Foreign Release Authority for the foreign release of classified information outside of an SIA/GSA. If the Requestor's Foreign Release Authority approves a release, the request should then be sent to dsp.international@defence.gov.au with a lead time of 15-20 business days for processing and final approval.

Table 1: Minimum Foreign Release Authority

Protective Marking	Official Information being shared under an SIA/GSA	Official Information being shared outside of an SIA/GSA
OFFICIAL	This information can be shared on a need-to-know basis No Foreign Release Approval required	This information can be shared on a need-to-know basis No Foreign Release Approval required
OFFICIAL: Sensitive	This information can be shared on a need-to-know basis, if Originator approval is granted No Foreign Release Approval required	EL1/O5 or equivalent in relevant Group/Service
PROTECTED	EL1/O5 or equivalent in relevant Group/Service	Initial Approval: EL2/O6 or equivalent in relevant Group/Service Final Approval: Director Strategic & International Security Policy
SECRET	EL2/O6 or equivalent in relevant Group/Service	Initial Approval: SES Band 1/One Star or equivalent in relevant Group/Service Final Approval: Assistant Secretary Security Policy & Services
TOP SECRET		

Note: *When determining the Foreign Release Authority for large compilations of Official Information or allowing access for extended periods of time, consideration is to be given to the aggregate classification in accordance with* ***DSPF Control 10.1 – Assessing and Protecting Official Information.***

Foreign Release Process

16. Where a legitimate business need has been identified to share Official Information with a Foreign Entity, the Requester is to follow the following foreign release process.

17. The Requester **must** complete the following three initial steps:

a. confirm the recipient receiving Official Information has a genuine need-to-know and, if necessary, holds an appropriate level of security clearance;

b. obtain written advice from the Originator approving the foreign release of the information;

(1) The Australian Department of Defence and Defence portfolio agencies treat Defence-originated information with no releasability caveat as equivalent to REL AUS/CAN/UK/NZL/USA; however, it is recommended Requesters obtain Originator approval for release.

(2) Jointly originated information requires written consent from all Originators prior to release

c. Determine whether the proposed foreign release is covered by an SIA/GSA.

18. If the release is covered by an SIA/GSA, follow the secondary steps as listed **Annex A**.

19. If the release is not covered by an SIA/GSA – either because it is outside the scope of an existing SIA/GSA or an SIA/GSA does not exist with the proposed Foreign Entity – follow the secondary steps as listed in **Annex B**.

a. A Risk Assessment **must** be completed as part of a foreign release of classified information outside of an SIA/GSA.

b. The recipient of information outside an SIA/GSA **must** also complete a commitment to protect this information.

20. If a Requester is unsure whether the proposed foreign release is covered by an SIA/GSA, they should contact Defence Security Division via dsp.international@defence.gov.au.

Dissemination of Information after Foreign Release Approval

21. Once approval has been granted by the Foreign Release Authority (and Defence Security Division if necessary), the information may be released in accordance with the approved scope and purpose.

a. Any additional security provisions imposed on the transmission of information outlined in the relevant SIA/GSA **must** be met.

b. Where an SIA/GSA does not contain specific transmission requirements for information, or the release is conducted outside of an SIA/GSA, physical transmission of Official Information is to be conducted according to the requirements set out in DSPF Control 71.1 - *Physical Transfer of Information and Assets*, and electronic transmission of Official Information is to be conducted according to the requirements set out in the *Australian Government Information Security Manual* and DSPF Control 27.1 – *Information Systems Data Transfer Security*.

Note: *The following text should be provided with any Official Information released to a Foreign Entity:*

This information remains the property of the Australian Department of Defence. Unauthorised communication and use of this information is a security incident and must be reported to the Australian originator, which may result in the limiting of your future access to Defence information and may be a serious criminal offence. If you have received this information in error, you are requested to contact the sender and delete it immediately.

Security Caveat Markings

23. Security caveats are additional markings applied to Official Information to indicate additional protections in addition to the security classification.

24. Releasability indicators, including 'Australian Eyes Only' ('AUSTEO') and 'Australian Government Access Only' ('AGAO'), are security caveats that permit or limit the release of Official Information to individuals based on citizenship or employment in the Australian Government, respectively. Refer to DSPF Control 10.1 *Classification and Protection of Official Information* for more information.

'Releasable to...' (REL)

25. The REL marking identifies information that has previously been approved for release to citizens of the indicated foreign countries or country grouping.

26. Information marked REL **must** only be released to citizens of the indicated foreign countries. For example, information marked REL AUS/USA cannot be shared with a UK citizen unless the Originator and Foreign Release Authority have provided approval in writing in line with the foreign release process outlined above. Once approval is received, the REL marking may be updated accordingly.

a. Where information is jointly produced by Australia and a foreign country, approval **must** be received from both countries prior to release to a third party.

27. Prior to release of information with a REL marking, any SIAs/GSAs with the listed foreign countries should be checked to confirm the intended release is within scope.

a. If there is a current and relevant SIA/GSA with the listed foreign countries, classified information may be released to appropriately cleared citizens or entities of those foreign countries without repeating the foreign release process.

b. If there is no existing SIA/GSA for the listed foreign countries or the release is outside the scope of the existing SIA/GSA, the process for information outside an SIA/GSA is to be followed as per **Annex B**.

Note:	*It is recommended Defence Security Division be engaged when stakeholders anticipate information is to be released outside of a SIA/GSA. Requests for assistance may be sent to dsp.international@defence.gov.au.*

28. Any security classified information approved for release under an SIA/GSA may have the releasability indicator followed by the appropriate country codes of the originating and receiving foreign countries added to the appropriate classification marking (e.g. SECRET REL AUS/USA). Further information on protective markings can be found in DSPF Control 10.1 *Classification and Protection of Official Information* and the Australian Government Security Caveat Standard.

a. REL markings should only to be applied to Australian-originated security classified information marked PROTECTED or above and **must** be stored, processed and transmitted on the DSN.

b. Foreign Information marked with a nationality-based releasability caveat **must** also be stored on the DSN.

(1) The Protective Security Policy Framework contains further information about the requirements for the storage, processing and communication of information marked with nationality-based releasability caveats.

Foreign national access to a Defence ICT system/network

29. Refer to DSPF Control 22.1 *Information and Technology Security (Personnel)* for the full application process for foreign national access to Defence ICT systems/networks.

30. Foreign Entity access to Defence ICT systems/networks without an appropriate Foreign Release Approval is a security incident and **must** be reported in accordance with DSPF Control 77.1 *Security Incident Management and Investigation*.

Key Definitions and Acronyms

1. **Foreign Entity.** A Foreign Entity is any organisation formed, registered or existing outside Australia, or an individual without Australian citizenship. This includes, but is not limited foreign governments, foreign companies, foreign non-government organisations, intergovernmental organisations, as well as foreign nationals whether they are located overseas or in Australia. Any individual not holding Australian citizenship is considered to be a foreign national for the purposes of this Control, including but not limited to contractors and subcontractors working for Australian companies with Defence Industry Security Program membership, and foreign exchange officers.

2. **Foreign Release Authority.** An APS or ADF official at a specified level/rank who holds an appropriate security clearance, and can make an informed decision about whether to approve or deny a foreign release request.

3. **GSA.** General Security Agreement. A treaty-level agreement between the governments of two or more countries, establishing conditions under which Official Information can be exchanged, protective marking standards and security classification equivalencies.

4. **Official Information.** Any information received, developed or collected by, or on behalf of, the Australian Government, by Defence personnel and person's engaged under a contract in their professional capacity. Includes classified information, not to be confused with information with the non-security classified marking OFFICIAL.

5. **Originator.** The entity that created the Official Information or on whose behalf the Official Information was created. An Originator can be a military or business unit within Defence, an Australian government department or agency, or a foreign entity.

6. **Requester.** The individual placing the request for Official Information to be released to a Foreign Entity. This includes but is not limited to ADF members, APS personnel, contractors and DISP members.

7. **SIA.** Security of Information Agreement/Arrangement. A treaty-level agreement or less-than-treaty-level arrangement between governments or government departments, establishing conditions under which Official Information can be exchanged, protective standards and security classification equivalencies.

Further Definitions

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

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

Annexes and Attachments

Annex A – *Foreign Release of Official Information – Under an SIA/GSA*.

Annex B – *Foreign Release of Official Information – Outside an SIA/GSA*.

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	7
Publication date	03 April 2024
Type of Control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Foreign Release of Official Information (Principle 15)
Related DSPF Control(s)	Classification and Protection of Official Information (Control 10.1) Information Systems (Personnel) Security (18.1) Defence Industry Security Program (16.1) Personnel Security Clearances (40.1) Security Incident Management and Investigation (77.1)
Related legislation	*Criminal Code Act 1995* (Cth)

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.
3	24 March 2020	AS SPS	Add note on escalation thresholds and refine foreign release process for REL caveated information. Clarify language and formatting for readability.
4	31 July 2020	AS SPS	Update to include Foreign National ICT Systems and Network access process in accordance with Control 18.1. Protective Marking update to align with PSPF
5	10 August 2020	AS SPS	Update hyperlinks to DSPF
6	14 July 2022	AS SPS	Revision of entire Control
7	04 April 2024	AS SPS	Updated for consistency of language regarding OFFICIAL: Sensitive becoming a classified information marking in the PSPF in August 2023

Defence Security Principles Framework (DSPF)

Annex A to DSPF Control 15.1 Foreign Release of Official Information
Foreign Release under an SIA/GSA

Foreign Release under an SIA/GSA

1. The following is applicable only when a foreign release is covered by an SIA/GSA.

2. After completing the initial steps found in paragraph 17 of DSPF *Control 15.1 – Foreign Release of Official Information*, the Requester **must**:

a. determine and submit the request to the appropriate Foreign Release Authority in their chain of command, including supporting documentation sufficient for an informed decision to be made regarding the foreign release.

(1) The supporting documentation should include the following:

(a) a statement outlining the scope of the release approval (e.g. is the approval for an individual document? Is all Official information up to a certain classification related to a specific operation/activity?);

(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 (e.g. is the information being released to an individual? Is it being released to a government/organisation?); and

(d) written advice from the Originator of the information that supports its release.

2. Once a foreign release request is received, the Foreign Release Authority should consider whether the information provided in the request is sufficient to justify a release and inform the Requester of their decision.

3. Appendix 1 provides a summarised workflow of the release process under an SIA.

Appendix

Appendix 1 - *Workflow for Foreign Release under an SIA/GSA*.

Document administration

Identification

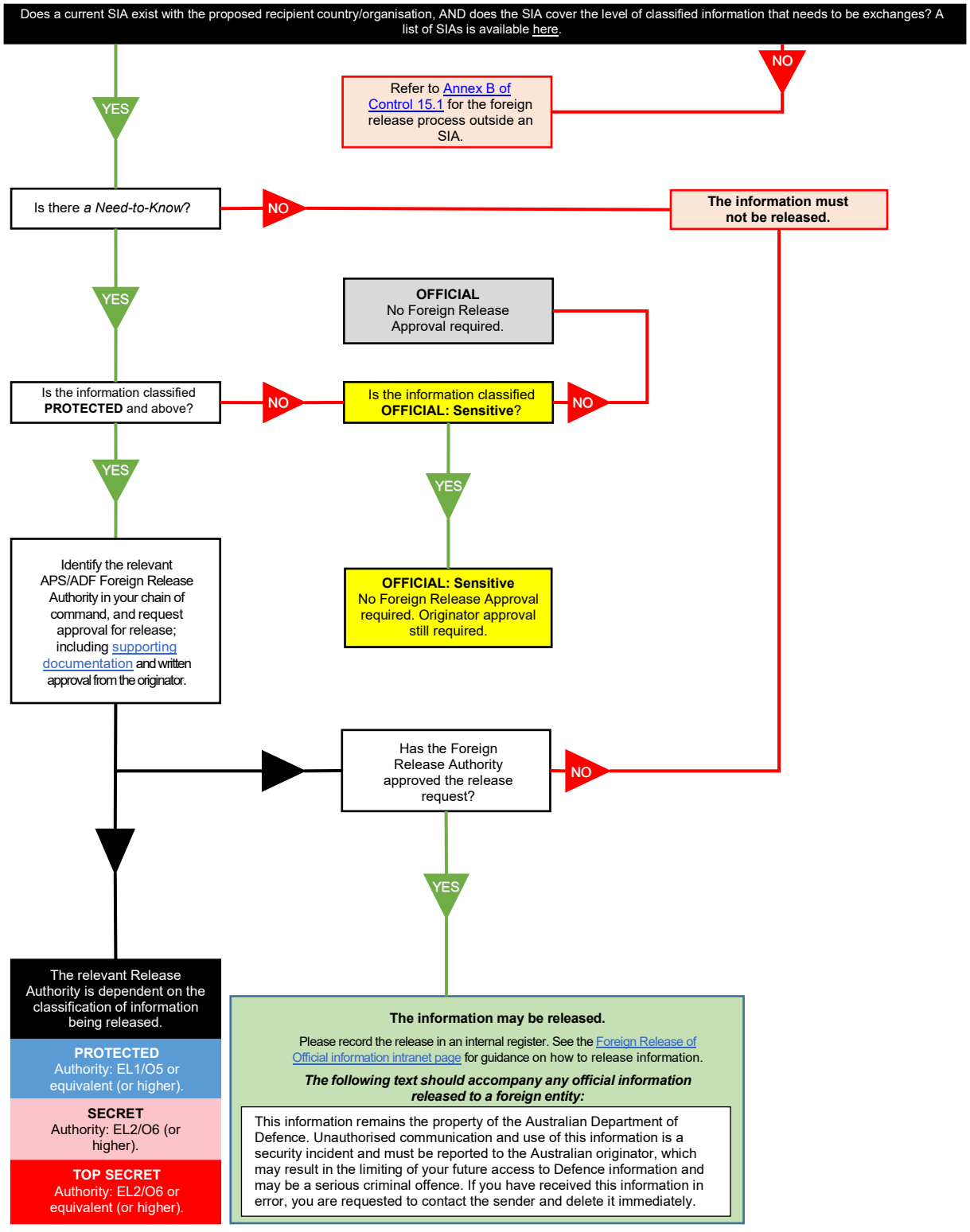
DSPF Annex	Foreign Release under an SIA/GSA
Annex Version	2
Annex Publication date	04 April 2024
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Foreign Release of Official Information
DSPF Number	15.1

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	14 July 2022	AS SPS	Created as part of the rewrite of Control 15.1 – Foreign Release of Official Information.
2	04 April 2024	D ISSP	Minor updates to Appendix 1 & 2 in accordance with FROI user guidance refresh

Appendix 1
Workflow for Foreign Release under an SIA/GSA



Defence Security Principles Framework (DSPF)

Annex B to DSPF Control 15.1 Foreign Release of Official Information
Foreign Release outside of an SIA/GSA

Foreign Release outside of an SIA/GSA

1. There may be circumstances where it may not be feasible to conclude a standing SIA/GSA for the one-off or ad hoc foreign release of classified information.

2. In those circumstances, after completing the initial steps found in paragraph 17 of *Control 15.1 – Foreign Release of Official Information*, the Requester **must**:

a. determine and submit the request to the appropriate initial Foreign Release Authority, including supporting documentation sufficient for an informed decision to be made about whether to endorse the foreign release.

(1) The supporting documentation should include the following:

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

(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 (e.g. 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 foreign release of classified information (see paragraph 6); and

(f) an outline of any proposed mitigation measures.

b. If endorsed by the initial Foreign Release Authority, the Requester **must** send the release request to the appropriate final Foreign Release Authority in

Defence Security Division by contacting dsp.international@defence.gov.au, who will make the final decision to approve or deny the request.

(1) Defence Security Division may seek further input from the initial Foreign Release Authority and Requester as part of this process.

3. If Defence Security Division provide final approval to release information, the Requestor **must** ensure the receiving Foreign Entity provides a written commitment to appropriately protect the shared information.

a. Defence Security Division have created the *Non-Disclosure Agreement Template* provided in Appendix 2 to this Annex to facilitate this.

(1) In circumstances requiring one-off or ad hoc foreign release of Official Information outside of an SIA/GSA, the Requester **must** ensure:

(a) the receiving official is notified in writing of the requirements for handling Australian information; and

(b) these requirements are acknowledged and accepted in writing by the receiving official.

(2) In exceptional circumstances, an exchange of emails prior to the provision of classified information, or signed acknowledgement of receipt of classified information by the receiving official, may suffice. Defence Security Division agreement should be sought in these circumstances.

(a) The exchange of emails should incorporate the relevant provisions of the *Template* outlining the protections in place for the information being released.

b. The release of classified information outside an SIA/GSA without Defence Security Division approval and without a written commitment from the receiving Foreign Entity is a security breach and **must** be reported.

4. The releasing area should maintain an internal register of all instances of foreign releases of Official Information outside of an SIA/GSA.

Formal risk assessment

5. A formal risk assessment is only required for foreign release of information conducted outside of an SIA/GSA that is marked PROTECTED and above, but may be used to provide additional assurance when conducting a foreign release inside an SIA/GSA.

a. The assessment could consider questions such as: what is the potential for the information to be compromised by misuse or unauthorised access –

intentional or unintentional – or unauthorised modification? If any of these things were to happen, what would the nature of the impact be to Australia's national security, Defence capability, and/or international relations?

6. Defence Security Division does not prescribe how a risk assessment should be developed; however, it is expected that Requesters and their chain of command provide evidence that the risks of sharing information outside of an SIA/GSA have been appropriately considered and addressed as required. Final release approval by the Release Authority will not be granted until a formal risk assessment is complete, in line with the Escalation Threshold.

7. The Security Risk Management page within the Defence Security Division intranet section contains guidance on conducting risk assessments, and a suite of security risk management tools.

Appendix

Appendix 1 – Workflow for the Release of Official Information Outside of an SIA/GSA

Appendix 2 – Non-Disclosure Agreement Template

Document administration

Identification

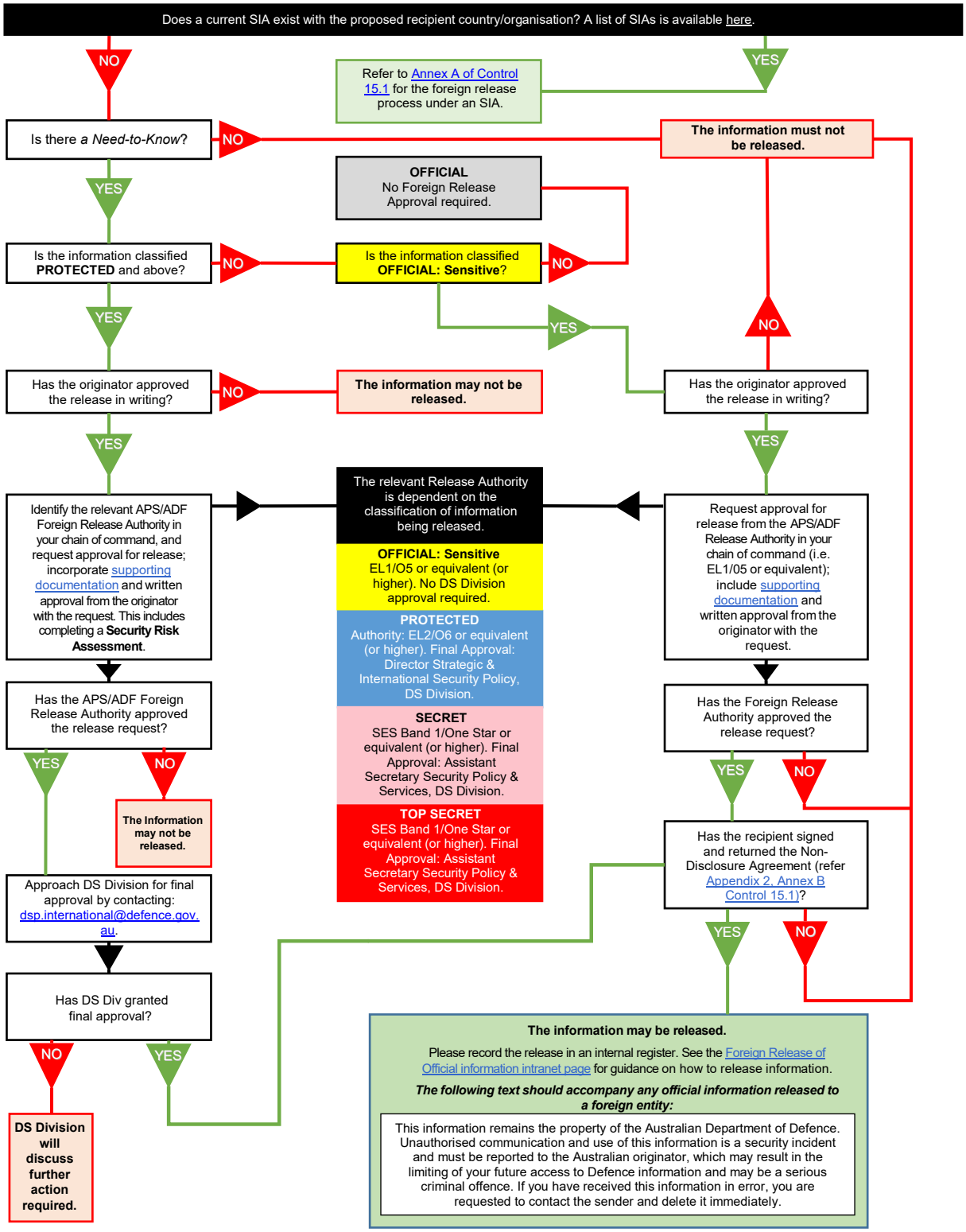
DSPF Annex	Foreign Release outside a SIA/GSA
Annex Version	2
Annex Publication date	03 April 2024
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Foreign Release of Official Information
DSPF Number	15.1

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	14 July 2022	AS SPS	Created as part of the rewrite of Control 15.1 – Foreign Release of Official Information.
2	03 April 2024	D ISSP	Minor updates to Appendix 1 & 2 in accordance with FROI user guidance refresh

Appendix 1 – Workflow for the Release of Official Information Outside of an SIA/GSA



Appendix 2 – Non-Disclosure Agreement Template

Non-Disclosure Agreement

In the absence of a Security of Information Agreement or Arrangement between Australia and Country/Department X, the Australian Department of Defence (ADOD) requests the acceptance of the following provisions to ensure the proper handling of Australian classified Information.

Recipient:	Name: Country: Official Position: Government Agency: Email: Phone:
Brief Description of the Classified Information:	E.g. Australian OFFICIAL: Sensitive instructive materials and ADOD "Defence PROTECTED Network" access.
Permitted Purpose:	E.g. Conduct of a secondment/project to [area] during [period].
Releasing ADOD Point of Contact (POC):	Name: Phone: Email:

Provisions

(1) The ADOD will provide the classified Information to the Recipient in accordance with Australian law and Whole-of-Government and departmental foreign release policies.

(2) After receiving the classified information, the Recipient will:

a) handle the information in a manner no less stringent than the requirements in Table 1 below;
b) only use the information for the Permitted Purpose, and not change its classification, except with the approval of the ADOD POC;

c) not disclose the information to any individuals who do not have a need-to-know, as well as unspecified third party National or Foreign Entities (including companies, foreign governments, or foreign nationals) without approval of the ADOD POC;
d) immediately notify the ADOD POC of any suspected or actual unauthorised or inadvertent disclosure of the information and take all practicable measures to minimise harm resulting from any disclosure;
e) return or destroy the information once no longer needed for the Permitted Purpose, and promptly notify the ADOD POC; and
f) ensure Recipient personnel do not access sites or ICT systems/networks which they have not been granted express permission to access by the ADOD.

(3) The ADOD will regularly audit the Recipient's use of Australian ICT systems/networks to ensure that any potential inappropriate use is captured. Delete if no ICT access sought.

Signature of this letter indicates acceptance of all provisions and handling requirements and a commitment that the Recipient will act in accordance with these provisions.

Failure to comply with any of these provisions could constitute a security breach/incident and lead to the termination of the Recipient's access to Australian classified information, sites and ICT systems/networks. It could also result in Recipient personnel in Australia being returned to their home country.

Signature below indicates acceptance of the above commitments on behalf of Country/Department X.

Country/Department X Defence Security Division preference is for an individual who is a manager/supervisor of the recipients of information to sign this Signature: Name: Title/position: Date:

Acknowledgement by the ADOD:

ADOD POC

Signature: Name: Title/position: Date:

Table 1 – Overview of minimum protection and handling requirements

The below table provides guidance on how the Recipient **must** handle the Classified Information.

Australian classification	**Protection and handling requirements**
OFFICIAL: SENSITIVE	**Access:** Personnel must have a 'need-to-know'. **Storage:** Minimum storage requirement in all areas is a lockable container. **IT:** Transmission is through a minimum of an Australian OFFICIAL network or encrypted public networks. The Recipient must also comply with the ADOD sponsoring area's Security Risk Assessment management plan and Standard Operating Procedures.
PROTECTED	**Access:** Personnel must have a 'need-to-know' and possess an appropriate personnel security clearance. **Storage:** PROTECTED information must be stored in a secure access controlled area and a safe. PROTECTED information may not be reproduced or stored electronically. The Recipient must also comply with the ADOD sponsoring area's Security Risk Assessment management plan and Standard Operating Procedures.

Defence Security Principles Framework (DSPF)

Defence Industry Security Program

General Principle

1. A secure and resilient defence industrial base is essential to meeting Australia's strategic objectives and maintaining the Department of Defence's (Defence) capability edge. Security risks associated with the procurement of goods and services need effective management to reduce the likelihood of increased security risk to Defence.

Rationale

2. Failure to consider and mitigate defence industry security risks could lead to compromised capability, operational failure, project delays and increased costs.

3. In addition to DSPF Principle 16, Defence uses DSPF Principles 11 – Security for Projects; 12 – Security for Capability Planning; and 82 - Procurement to support industry to improve their security posture and support industry to ensure Defence capability is underpinned by a strong security culture and secure workforce.

4. Defence also uses Whole-of-Government initiatives and frameworks to consider and mitigate security risks.

Expected Outcomes

5. Defence is assured that goods and services are delivered uncompromised. Accountabilities and responsibilities for security risk management are understood and suitable risk reduction activities are applied to effectively manage industry security risks.

6. Australia's Defence industry sector is well positioned to be a trusted partner in the global defence supply chain.

Escalation Thresholds

Risk Rating	Responsibility
Low	Assistant Director DISP Policy
Moderate	Director DISP Application Management
Significant	Assistant Secretary Defence Industry Security
High	First Assistant Secretary Defence Security
Extreme	Defence Security Committee (Chair) – through Assistant Secretary Defence Industry Security

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

Document Administration

Identification

DSPF Principle	Defence Industry Security
Principle Owner	First Assistant Secretary Defence Industry Security
DSPF Number	Principle 16
Version	8
Publication date	29 January 2026
Releasable to	Defence, Defence Industry and Public
Underlying DSPF Control/s	Control 16.1 – Defence Industry Security Program
Control Owner/s	Assistant Secretary Defence Industry Security

Related Information

Government Compliance	**Protective Security Policy Framework (PSPF):** PSPF Annual Release **Legislation**: *Privacy Act 1988* (Cth) **Standards**: AS: 4811-2022: Workforce screening
Read in conjunction with	Security for Projects Security for Capability Planning; and Procurement
See also DSPF Principle(s)	Classification and Protection of Official Information Foreign Release of Official Information Information Systems (Physical) Security Information Systems (Personnel) Security Information Systems (Logical) Security Cyber Security Assessment and Authorisation Personnel Security Clearance Temporary Access to Classified Information and Assets Physical Transfer of Information and Assets
Implementation Notes, Resources, and Tools	Defence Industry Security Program webpage AGSVA Resources

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
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	17 February 2022	FAS DS	Enhancements to Defence Industry Security Program to improve the uplift of industry security and engagement
5	23 September 2022	FAS DS	Updates to Escalation Thresholds and Government Compliance
6	24 November 2023	FAS DS	Transfer of Control Ownership from AS SPS to AS DIS
7	27 September 2024	FAS DS	Update to “Related information” and to the Escalation Threshold table.
8	29 January 2026	FAS DS	Updated title, ‘releasable to’ and hyperlinks

Defence Security Principles Framework (DSPF)

Defence Industry Security Program

Control Owner

1. The Assistant Secretary Defence Industry Security (AS DIS) is the owner of this Control.

Escalation Thresholds

2. AS DIS 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	Assistant Director DISP Policy
Moderate	Director DISP Application Management
Significant	Assistant Secretary Defence Industry Security (AS DIS)
High	First Assistant Secretary Defence Security (FAS DS)
Extreme	Defence Security Committee (Chair) – through AS SPS

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

About the Defence Industry Security Program

3. Security is critical to the resilience of Defence systems, information, assets and our people. Defence industry partners' ability to meet their security obligations and enhance their resilience is critical to protecting the government's investment in secure, uncompromised Defence capability.

4. The Defence Industry Security Program (DISP) is one control in a layered approach to security that contributes to strengthening the assurance that the government's significant investment in Defence capability is appropriately protected. Managed by the Defence Industry Security Branch (DISB), the DISP:

a. is a membership-based program that sets baseline security requirements for Industry Entities wishing to engage with Defence;

b. supports industry to identify security risks and to understand and apply security controls across the domains of governance, personnel security, physical, and information and cyber security;

c. includes a system of reviews to ensure continued compliance; and

d. enhances Defence's ability to monitor and mitigate security risks.

5. DISP membership is **mandatory** for Industry Entities who:

a. require access to classified information or assets PROTECTED and above;

b. supply, maintain, store or transport weapons or explosive ordnance;

c. provide security services for Defence bases or facilities;

d. are Australian Community Members under the Australia-US Defence Trade Cooperation Treaty; and/or

e. are required to hold a DISP membership as a condition of a Defence contract.

6. The exception to this requirement is where:

a. an Industry Entity's personnel are handling classified information within Defence facilities and using Defence assets and ICT networks (refer to *DSPF Principle 74 – Access Control*).

b. an Industry Entity has accreditation recognised under a Security of Information Agreement or Arrangement (SIA) or Government Security Agreement (GSA) with an international partner (refer to *DSPF Principle 15 – Foreign Release of Official Information*).

7. DISP members who participate in Special Access Programs must also comply with the conditions in Annex C – Special Access Programs.

8. Defence Officials undertaking procurement and managing contracts (Contract Managers), **must** stipulate whether DISP membership is a requirement, and specify the level of membership the Industry Entity should hold, in tendering and contracting documentation.

9. The AS DIS is the responsible decision maker for determining whether to approve, deny, limit, downgrade, suspend or terminate an Industry Entity's DISP membership.

Membership levels

10. DISP membership is defined by levels across the security domains of: governance, personnel, physical, and information and cyber security.

11. DISP has four membership levels within each security domain that align with Australian Government security classifications and determine the level of information an Industry Entity is accredited to handle:

	Governance	Personnel Security	Physical Security	Information and Cyber Security
Entry Level	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive	OFFICIAL / OFFICIAL: Sensitive
Level 1	PROTECTED	PROTECTED (Baseline)	PROTECTED	PROTECTED
Level 2	SECRET	SECRET (NV1)	SECRET	SECRET
Level 3	TOP SECRET	TOP SECRET (NV2)	TOP SECRET	TOP SECRET

12. Industry Entities can apply for different membership levels across each domain based on their demonstrated business requirements.

13. An Industry Entity's governance membership level **must** be equal to the highest level applied for across the other three domains.

14. On initial application to join the DISP, Industry Entities can only apply for DISP 'Entry Level' membership for the Information and Cyber Security domain, unless they have existing certification and accreditation provided by Joint Capabilities Group (Defence Cyber and Information Assurance Branch (DCIAB)) or an explicit requirement to fulfil a current Defence contract. Higher information and Cyber Security levels may be applied for through DCIAB once DISP membership has been granted. Industry Entities who need to apply for Level 1 membership or higher will need to seek Assessment and Authorisation under *DSPF Principle 23.1 – Cyber Security Assessment and Authorisation*.

15. Industry Entities without a Defence contract, who are seeking to position themselves to enter the Defence supply chain, should apply for Entry Level membership across all domains. Industry Entities applying for Levels 1, 2 and 3 membership **must** provide an appropriate justification to support higher levels of membership (such as working on highly classified programs/projects).

DISP membership

16. DISP membership is open to any Australian business looking to become a part of the Defence industry supply chain. You do not require a contract with Defence to become a member of DISP.

17. DISP membership is not automatic. On receipt of an Industry Entity's completed application, Defence will conduct an assessment of the Industry Entity's eligibility and suitability for DISP membership.

18. To be eligible for DISP membership, the Industry Entity, **must** as a minimum:

a. be registered as a legal business entity in Australia (i.e. has an ABN or ACN);

b. be financially solvent (not under administration or receivership);

c. have a director or senior executive able to obtain an Australian Personnel Security Clearance (commensurate with the level of DISP membership) and fulfil the role of Chief Security Officer (CSO);

d. have a staff member able to obtain an Australian Personnel Security Clearance (commensurate with the level of membership) and fulfil the role of Security Officer (SO) (the CSO and SO can be the same individual);

e. establish and be able to maintain, the security standards for their requested level of membership (refer to *Annex A*);

19. Defence will also consider the following when assessing an Industry Entity's eligibility:

a. any risks arising from an Industry Entity's previous or current commercial activities with any listed terrorist organisation or entity linked to any listed terrorist organisations (as listed under the *Criminal Code Act 1995* (Cth)), or to persons for mercenary, terrorist or other criminal activity;

b. any relationships with regimes subject to Australian sanctions laws including the United Nations Security Council sanctions regimes and Australian autonomous sanctions regimes; and

c. any relationship with persons and/or entities on the Department of Foreign Affairs and Trade Consolidated List.

20. An Industry Entity that meets the eligibility requirements can apply for DISP membership through the DISP Member Portal.

21. DISB may request additional information and/or documentation from the Industry Entity to confirm eligibility. Where such material is not provided within 75 days, the DISP application will become inactive until further information is received.

22. DISP applicants and members **must** have a centralised point of contact email (not attached to an individual person) in the form of "DISP@company domain name". Web-based mail services such as Google, Yahoo, AOL, Yandex etc. will not be accepted. While DISP accepts variations (such as .com.au, .com, .biz, or .net), all email systems used for DISP membership **must** be hosted in Australia. This email account **must** remain current and be monitored on a regular basis. This email address will be the means by which DISB corresponds with Industry Entities in relation to their DISP membership.

23. Applicants without an ABN or ACN are not eligible for DISP membership. However, they may be able to participate in classified contracts if they are recognised under an SIA or GSA with an international partner (refer to *DSPF Principle 15 – Foreign Release of Official Information*).

24. Contract Managers **must** notify DISB when Defence engages (via contract, panel, or partnership) an Industry Entity requiring DISP membership, when DISP membership is required as a condition of a Foreign Investment Review Board decision, or when contractual security requirements have changed, through the Notification of Engagement Requiring DISP Membership Portal.

Suitability considerations

25. On receipt of a completed application, DISB will assess the Industry Entity's suitability for DISP membership. Additional information and/or documentation may be required from the Industry Entity to determine its suitability and the level of support the Industry Entity may require to meet DISP requirements.

26. As part of the application assessment process, Defence undertakes the following assessment activities:

a. personnel security checks of nominated security staff;

b. an assessment of an Industry Entity's cyber maturity;

c. an Entry Level Assessment (ELA) to confirm that the Industry Entity has in place appropriate security governance and risk documentation;

   i. The ELA is designed to confirm an Industry Entity meets the *DISP Membership Level Requirements* as described in *Annex A*. This Annex outlines the requirements for each membership level and security domain.

d. Security Officer training for nominated security staff;

e. Foreign Ownership, Control and Influence (FOCI) checks;

f. Physical accreditation (depending on membership level);

g. ICT accreditation by DCIAB (depending on membership level); and

h. An interview with the SO/CSO to confirm their understanding of their security obligations.

27. Defence may also consider the following when assessing an Industry Entity's application:

a. any significant risks arising through the Industry Entity's reliance on international supply chains;

b. any risks arising through an Industry Entity's exposure to criminal and other unlawful activities;

c. any risks arising from an Industry Entity's previous or current commercial activities with states that have policies or strategic interests inconsistent with those of Australia or our allies; and

d. any other consideration that Defence considers relevant to the Industry Entity's suitability to hold DISP membership.

28. Industry Entities will not be granted DISP membership until they can demonstrate the security standards appropriate to their nominated levels.

29. Where an Industry Entity does not meet the security requirements for the level of membership selected, Defence may require the Industry Entity to enter an uplift and remediation program to assist compliance with DISP security obligations.

30. Once an Industry Entity has met the eligibility and suitability requirements, DISP membership will be granted in the form of a DISP Membership Certificate.

Refusing DISP membership

31. An application for DISP membership will be refused if Defence is reasonably satisfied that eligibility and suitability criteria are not met, or if there are concerns that granting membership would not be in Defence's interest or in the national interest.

DISP membership fees

32. There are no DISP membership fees, however, Industry Entities are responsible for covering the costs associated with meeting and maintaining the standards for their level of DISP membership.

Ongoing DISP membership requirements

33. DISP membership is ongoing provided members continue to meet their obligations under the program.

Ongoing security obligations

34. As DISP members, Industry Entities are responsible for safeguarding Defence information, assets, material and systems. DISP members **must**:

a. comply with contemporary Australian Government and Defence security legislation and policies. This includes achieving and maintaining the standards required by the DSPF, the Protective Security Policy Framework (PSPF), and the Information Security Manual;

   i. universities and research institutions may also need to comply with *DSPF Control 31.1 - Defence Research, Innovation and Collaboration Security (DRICS)*;

b. report all security and cyber security incidents in accordance with *DSPF Control 77.1 – Security Incidents and Investigations* and *DSPF Control 24.1 – Information and Technology Security (Incident Management)*; and

c. complete an Annual Security Report (ASR).

Ongoing reporting obligations

35. As DISP members, Industry Entities **must** report to DISB all changes that might impact their membership, including (but not limited to):

a. eligibility changes (including with regard to ownership or control);

b. other changes in circumstances (such as change of contact details); and

c. changes to the Industry Entity's CSO and SO.

DISP uplift, remediation and assurance program

36. DISB manages an active assurance and uplift program to assist Industry Entities to meet and maintain their security obligations under DISP, including:

a. ASRs on the anniversary of the Industry Entity's membership grant. The ASR **must** be signed by the CSO and submitted via the DISP Member Portal

b. Ongoing Suitability Assessment (OSA) 'desk top' audits to confirm that members are continuing to meet their security obligations. OSA selection is an outcome of an internal risk-based framework.

c. Deep-Dive Audits (DDA) ascertain the extent of compliance with required policies and procedures, including inspections of documents, as well as identify areas of potential improvements to manage governance, personnel, physical and cyber security risks.

37. A condition of DISP membership is that members **must** engage with uplift, remediation and assurance activities conducted by Defence (or a third party nominated by Defence) and provide requested security artefacts to support Defence assurance activities.

38. Industry Entities must implement recommendations from DISP uplift, remediation and assurance activities within a mutually agreed timeframe. Defence may vary, suspend or terminate DISP membership if the DISP member fails to implement the recommendations within the agreed timeframe.

Non-compliance

39. Defence is committed to supporting Industry Entities to meet and maintain their obligations as DISP members. Where an Industry Entity fails to meet the requirements of their membership, Defence will employ a scalable approach in responding to the non-compliance.

Escalation pathway

40. Where non-compliance occurs, Defence will seek an informal resolution with the Industry Entity, where appropriate. If an informal approach is unsuccessful, Defence may seek a number of formal remedies, including – but not limited to:

a. providing formal advice to the Industry Entity to address the non-compliance and prevent future non-compliance (or any precursor activities to non-compliance);

b. requiring a DISP member to take specific actions (with supporting evidence of implementation);

c. requiring additional security reporting from the DISP member and imposing additional compliance monitoring activities;

d. limiting , downgrading, suspending or terminating DISP membership; and

e. triggering breach of contract clauses where the DISP member is engaged in contracts with Defence.

41. DISB will consult with Contract Managers who hold a contract with the affected Industry Entity before making a determination to limit, downgrade, suspend or terminate DISP membership.

Limiting DISP membership

42. An Industry Entity may be restricted to a specified membership level for governance, personnel, physical, and/or information and cyber security when applying for DISP membership. Defence will work with the DISP member to establish the limits to be applied subject to the nature of the security risk and potential implications of the non-compliance.

Downgrading DISP membership

43. An Industry Entity may have their membership level downgraded across one or more of the membership categories. In such cases, all entitlements, certifications and accreditations at the membership levels held by the DISP member will be revoked.

Suspending DISP membership

44. DISP membership may be suspended following an assurance activity or security investigation which identifies non-compliance or security control breaches. This suspension may affect current contracts and prevent the DISP member from entering into additional contracts that require DISP membership with Defence until the issues leading to the suspension are rectified.

Termination of DISP membership

45. If DISP membership is terminated, the Industry Entity will not be able to provide any services to Defence that require DISP membership. This includes storing or transporting Defence weapons or explosive ordnance; providing security services for Defence bases and facilities; any other Defence-related activity requiring secure-handling, or a service that requires DISP membership as a condition of a contract.

46. When DISP membership is suspended, withdrawn or terminated, an Industry Entity will no longer be able to:

a. hold Defence-sponsored Personnel Security Clearances for the CSO and SO;

b. sponsor new and current Personnel Security Clearances;

c. receive security classified information, materials or assets;

d. continue to hold classified information, assets and materials belonging to Defence (in line with contract terms and conditions and *DSPF Control 10.1 Classification and Protection of Official Information*);

e. engage in Defence projects requiring DISP membership;

f. continue Defence work at the facility where the security risk/breach occurred (where physical or ICT certification and accreditation has been deactivated); and/or

g. use any DISP membership branding.

Procedure for membership modification by DISP member

47. A DISP member may apply in writing to upgrade or downgrade their DISP membership levels at any time as appropriate for their business requirements, or in order to meet contractual requirements.

48. When seeking to upgrade their DISP membership, Industry Entities will need to undergo an additional suitability assessment. Industry Entities will need to submit an *AE250 form* and include an appropriate justification for an upgrade. Requests for upgrades without an appropriate justification will not be considered.

a. A suitability assessment may not be required for voluntary downgrading of membership levels where the DISP member can demonstrate compliance with the new level/s.

49. Defence will confirm the change in membership with a revised DISP Membership Certificate and notify relevant Contract Managers.

Voluntary suspension or withdrawal from DISP

50. DISP members can voluntarily suspend or cancel their DISP application or membership at any stage by contacting DISP.info@defence.gov.au.

Procedural Fairness

51. Procedural fairness applies to a decision to deny, limit, downgrade, suspend or terminate DISP membership. Procedural fairness ensures that a fair and reasonable procedure is followed when making a decision that may adversely affect an Industry Entity's DISP application for membership or current membership. If Defence intends to make a decision which may adversely affect an Industry Entity, the Industry Entity will have a reasonable opportunity to respond in writing before a final decision is made.

Appeals and reviews

52. If an Industry Entity receives notification that their DISP membership application has not been approved or that their DISP membership has been limited, downgraded, suspended or terminated, the Industry Entity can ask for a review of the decision. Defence Security Division will inform the Industry Entity of the relevant avenue(s) of appeal when notifying them of an adverse membership decision.

Roles and responsibilities

Defence

53. In the administration of DISP, Defence has a responsibility to:

a. act in good faith;

b. act in the national interest;

c. provide services to certify and accredit facilities and ICT networks (refer to *DSPF Principle 23 – Cyber Security Assessment and Authorisation*, and *Principle 73 – Physical Security Certification and Accreditation*) in support of a DISP membership;

d. provide vetting services through the Australian Government Security Vetting Agency (AGSVA) in support of a specific requirement for a DISP membership; and

e. uphold responsibilities under Commonwealth and Defence policy.

Defence Industry Security Branch

54. DISB is responsible for the operations and management of DISP, including, but not limited to:

a. providing information and support to Industry Entities wishing to join the DISP;

b. processing DISP membership applications;

c. providing ongoing security management advice; and

d. undertaking uplift, remediation and assurance processes associated with membership obligations and security requirements.

55. DISB will advise Contract Managers who have completed a Notification of Engagement Requiring DISP Membership of any changes in DISP member profiles during the life of a contract.

56. DISB will also notify Contract Managers of non-compliance with DISP obligations, including if Industry Entities:

a. do not provide required information in response to an audit request within a 28 business day period;

b. have not met assurance reporting requirements; and/or

c. have not implemented assurance remediation recommendations within agreed timeframes.

57. Where DISP membership is required by Defence in a tender or contract, DISB will provide Contract Managers with details regarding the DISP member sought for engagement. This includes confirmation of the DISP member's membership status and membership levels. Contract Managers are to consider the information provided to assess whether the DISP member is suitable for engagement.

Contract Managers

58. Contract Managers **must** stipulate whether DISP membership is a requirement, and specify the level of membership the Industry Entity should hold, in tendering and contracting documentation.

59. Contract Managers **must** notify DISB when engaging (via contract, panel, or partnership) an Industry Entity requiring DISP membership, when DISP membership is required as a condition of a Foreign Investment Review Board decision, or when contractual security requirements have changed.

60. Contract Managers should notify DISB of any significant updates in relation to current engagements with a DISP member, including incidents of non-compliance with DISP obligations.

Industry Entities

61. Industry Entities applying and participating in DISP are responsible for:

a. acting in good faith;

b. ensuring information provided is not deceptive or misleading;

c. applying the 'need-to-know' principle (including for cleared individuals within the Industry Entity itself);

d. disclosing, and making available to Defence, all relevant and required information/artefacts as requested;

e. meeting all security requirements specified by Defence, and any Australian Commonwealth Government Entity (including ensuring no unauthorized access to official and classified information, assets, materials and systems); and

f. complying with all other obligations applicable to their DISP membership, including but not limited to:

   i. engaging with assurance activities, such as ASRs, OSAs, and DDAs;

   ii. providing required information and/or any other requirements to support DISP assurance and remediation activities; and

   iii. maintaining communication with DISB.

Chief Security Officer

62. An Industry Entity's CSO **must** be able to obtain and maintain a Personnel Security Clearance commensurate with the Industry Entity's level of DISP membership.

63. The CSO is the authority for the Industry Entity's security posture and is responsible for the oversight of security arrangements and championing a positive security culture. They have the flexibility to delegate the day-to-day management of protective security to the SO/s where required (the CSO and SO can be the same person).

64. The CSO **must** be a director or senior executive with the ability to implement policy and direct resources to meet security requirements.

65. The CSO is required to complete the *DISP Security Officer Training* course as part of the application process, and every three years thereafter.

66. The CSO is accountable for ensuring:

a. all obligations contained in this policy and other supporting documents for the Industry Entity's level of membership are met;

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

c. DISP reporting obligations are fulfilled;

d. official and classified materials entrusted to the Industry Entity are protected in accordance with DSPF requirements at all times;

e. the DISP ASR is completed by the Industry Entity and agreed to by the executive (Board equivalent), all recommendations are implemented within the agreed timeframes, and the ASR is provided to Defence annually on the anniversary of the membership grant; and

f. any change in the Industry Entity's circumstances that may impact their ability to maintain DISP membership (including changes in ownership and control) is reported to Defence (refer to *Annex B*).

67. The Industry Entity **must** notify Defence in writing of any changes to the CSO or SO within 14 business days of the change.

Security Officer

68. Industry Entities may appoint multiple SOs in accordance with their operational footprint. All SOs **must** comply with the requirements of DISP membership.

69. An Industry Entity's SOs **must** be able to obtain and maintain a Personnel Security Clearance commensurate with the Industry Entity's level of DISP membership. Where an Industry Entity holds Level 3 DISP membership, SOs with limited security responsibilities may hold lower level Personnel Security Clearances. Industry Entities **must** document in their security policies and plans the roles and responsibilities of SOs that hold lower level Personnel Security Clearances.

70. In order to obtain authority to sponsor and manage Personnel Security Clearances within the Industry Entity, an SO **must** have a minimum Negative Vetting 1 (NV1) Personnel Security Clearance. SOs cannot sponsor Personnel Security Clearances at a level higher than the Personnel Security Clearance level they hold (e.g. an NV1 clearance holder cannot sponsor NV2 clearances).

71. An SO is required to complete the *DISP Security Officer Training* course as part of the application process, and every three years thereafter. SOs **must** also undertake any additional required training associated with the SO position. An SO is responsible for:

a. the development and application of security policies and plans for their Industry Entity;

b. ensuring sensitive and classified materials entrusted to the Industry Entity are protected in line with DSPF requirements at all times;

c. ensuring and facilitating Defence mandated security education and training courses for Industry Entity personnel engaged in Defence work;

d. implementing arrangements and training for insider threat identification, reporting and management;

e. reporting security and fraud incidents, and contact reports, in accordance with *Control 77.1 – Security Incidents and Investigations*;

f. maintaining a Designated Security Assessed Position list, which is to be made available to Defence upon request (refer to *Annex A*). (The Protective Security Policy Framework mandates that Industry Entities identify and record positions that require a security clearance and the level of clearance required);

g. where relevant, sponsoring and managing all Personnel Security Clearances issued under the authority of the Industry Entity's DISP membership in accordance with the *DSPF Control 40.1 – Personnel Security Clearances*;

    i. An SO **must** actively monitor and manage the ongoing suitability of sponsored security cleared personnel including their security attitudes and behaviours;

    ii. An SO **must** notify AGSVA when a clearance holder no longer requires their clearance or when they separate from the DISP Industry Entity;

    iii. Personnel Security Clearances requiring an eligibility waiver **must** be approved by Defence. Refer to *DSPF Control 40.1 – Personnel Security Clearances* for exceptional circumstances criteria; and

    iv. Positive Vetting clearances can only be sponsored by the authorities outlined in *DSPF Control 40.1 – Personnel Security Clearances*.

72. Where an Industry Entity or CSO/SO fails to meet these requirements, Defence may vary, suspend or terminate the Industry Entity's DISP membership.

Defence Industry Security Program Privacy Notice

73. Defence undertakes checks to assess an Industry Entity's suitability to hold and maintain DISP membership in accordance with Control 16.1 in the DSPF. This involves collecting, using and disclosing personal information to Defence capability managers, contract managers, project leads and other Australian Government departments and agencies.

74. DISB respects your company's confidential information and the personal information of individuals who are associated with your company. DISB complies with the Australian Privacy Principles (APPs) in Schedule 1 to the *Privacy Act 1988*, which govern the handling of personal information (including sensitive information) for the efficient and effective administration of the DISP. DISB also operates in line with the Department of Defence's APP privacy policy under APP 1.3. A copy of the DISP Privacy Notice can be found here.

Appropriate use of DISP branding

75. Defence has a range of emblems and logos that are protected by legislation. Permission to use Defence logos and emblems is managed by Defence Branding. Permission from Defence **must** be sought before using all Defence logos and emblems, including DISP branding.

Additional Resources

Resource	Description
Australian Standard (AS):4811-2022 – Workforce Screening now incorporates Australian Standard International Organisation for Standardisation (AS ISO) 31000:2018 (both available for purchase on the Standards Australia website).	This is the Australian standard for workforce screening. Workforce screening applies to security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources. Requirements under the standard include: • An identity check requiring 100 points of ID • Address history checks for a minimum of five years • Character reference checks • A current national police check • An ASIC check (where relevant) • Checks on all declared experience and qualifications
Criminal Code Act 1995 (Commonwealth)	The *Criminal Code Act 1995* provides an integrated and coherent statement of the major offences against Commonwealth law. The statement of general principles is exhaustive; the principles apply to all Commonwealth offences, whether or not they are included in the *Criminal Code*.
Cybercrime Act 2001 (Commonwealth)	The *Cybercrime Act 2001* updates existing Commonwealth provisions on computer-related crime. The Act outlines main offences relating to computer-related crime, including: • Unauthorised access, modification or impairment to commit a serious offence • Unauthorised modification of data to cause impairment • Unauthorised impairment of electronic communication

	• Unauthorised access to or modification of restricted data • Unauthorised impairment of data held on a computer disk, credit card or other data storage device • Possession of data with intent to commit a computer offence • Production, supply or obtaining of data with intent to commit a computer offence
Defence Privacy Policy	The Defence Privacy Policy is designed to inform individuals about the way Defence collects, stores, uses and discloses personal information. This policy provides guidance about how you can access, or seek correction of, personal information held by Defence.
Defence Security Principles Framework (DSPF)	The DSPF is the primary security framework for Defence to manage security risk.
Essential Eight Maturity Model	The Essential Eight Maturity Model supports the implementation of the Australian Signal Directorate's (ASD) Essential Eight risk mitigation strategy. It is based on ASD's experience in producing cyber threat intelligence, responding to cyber security incidents, conducting penetration testing and assisting organisations to implement the Essential Eight.
Information Security Manual	A cyber security framework that organisations can apply, using their risk management framework, to protect their systems and data from cyber threats.
National Legislation Amendment (Espionage and Foreign Interference) Act 2018 (Commonwealth)	The *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018* criminalises covert and deceptive activities of foreign actors that intend to interfere with Australia's institutions of democracy, or support the intelligence activities of a foreign government.

Privacy Act 1988 (Commonwealth)	The *Privacy Act 1988* was introduced to promote and protect the privacy of individuals and to regulate how Australian Government agencies and organisations handle personal information. The Act includes 13 Australian Privacy Principles (Schedule 1), which apply to some private sector organisations as well as most Australian Government agencies.
Protective Security Policy Framework (PSPF)	The PSPF assists Australian Government entities to protect their people, information and assets, both at home and overseas. It sets out government protective security policy and supports entities to effectively implement the policy across the following outcomes: • Security governance • Information security • Personnel security • Physical security
Public Service Act 1999 (Commonwealth)	The *Public Service Act 1999* governs the operation of the Australian Public Service, and is supported by subordinate legislation: • *Public Service Regulations 1999* • *Public Service Classification Rules 2000* • *Australian Public Service Commissioner's Directions*
Australia-US Defence Trade Cooperation Treaty	The Treaty provides a framework for the export and transfer of controlled goods between Australia and the US within an Approved Community without the need for an export license.

Key Definitions

76. **Australian Community Members**. Australian Government and non-government entities that have been approved to be members of the Approved Community in accordance with the Australia-US Defence Trade Cooperation Treaty.

77. **Australian Government Security Vetting Agency (AGSVA).** AGSVA is the central vetting agency for the Australian Government and conducts security clearance assessments for federal, state and territory agencies.

78. **Chief Security Officer (CSO).** A role occupied by a senior executive in an Industry Entity that is responsible for the oversight of, and responsibility for, security arrangements and championing a positive security culture.

79. **Contract Manager.** For the purposes of this policy, Contract Managers are defined as Defence officials responsible for conducting procurement and managing contracts; this could include but is not limited to Program Managers, Project Managers, Senior Project Officers, Project Officers or any other role with contracting responsibilities.

80. **Cyber Assurance Program.** A program managed by the DISB to assist DISP members with meeting their ongoing security obligations, including eligibility assessments, cyber assessments and uplift, annual self-reporting, Ongoing Suitability Assessments and Deep-Dive Audits.

81. **Decision Maker.** The Assistant Secretary Defence Industry Security (AS DIS) is the DISP Control Owner and, for the purposes of this policy, AS DIS will normally be the original decision maker for the purpose of determining whether or not to refuse, limit, downgrade, suspend or terminate an affected party's DISP membership. In the event AS DIS is conflicted or otherwise unavailable or unable to act as a Decision Maker, the Decision Maker will be the person appointed in writing by AS DIS to act as such.

82. **Defence Industry Security Branch (DISB).** DISB is responsible for the processing of DISP membership applications and undertaking the assurance and remediation processes associated with membership obligations and security requirements. DISB is also responsible for the ongoing assurance framework for DISP members, once admitted into the program.

83. **Defence Industry Security Program (DISP)**. A vetting and assurance program that supports Defence industry to improve their security posture for the purpose of engaging in Defence projects, contracts and tenders.

84. **Deep-Dive Audit (DDA)**. Deep-Dive Audits seek to provide an independent review of whether DISP members are continuing to meet ongoing security requirements commensurate with their level of membership. DISB audits involve interviews with Security, HR and IT staff, reviewing a company's security

policies and plans, personnel, information and physical security arrangements and security registers, including physical security inspections.

85. **Designated Security Assessed Positions (DSAP)**. A Designated Security Assessed Position (DSAP) is a position that has been assessed by the DISP Industry Entity as requiring access to sensitive or classified information, materials and assets. A DSAP list identifies each position within an Industry Entity that requires a security clearance, the level of clearance required for each of those positions, and details of occupants of the positions. Maintaining a list of security assessed positions ensures that access to classified materials is appropriately monitored and managed.

86. **Eligibility**. Criteria outlining Industry Entity eligibility to apply for DISP membership, including legal operating status as an Australian business and ability to maintain the security standards for their requested level of membership.

87. **Industry Entity**. An Industry 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.

88. **Entry Level Assessment (ELA)**. An assurance activity to validate that information provided in the application is supported by evidence, and that the Industry Entity has in place the required security controls commensurate with the level of DISP membership sought.

89. **Foreign Ownership, Control and Influence (FOCI)**. Where a foreign interest has direct or indirect power, whether or not exercised, to direct or decide matters affecting the management or operations of the company.

90. **Ongoing Suitability Assessment (OSA)**. The OSA is a ‘desk top’ audit to confirm that members are continuing to meet their security obligations. OSA selection is an outcome of an internal risk-based framework. The OSA aims to increase awareness and enhance security policies, procedures and risk management strategies DISP members have in place. Where opportunities for improvement are identified, recommendations are provided to members to assist in uplifting their security policies and practices, ensuring that Defence and Defence industry continues to protect personnel, information and assets.

91. **Personnel Security Clearance**. A series of assessments into an individual’s suitability to have ongoing access to security classified resources. The purpose is to determine whether an individual possesses and demonstrates an appropriate level of integrity (a range of character traits) that indicate the individual is able to protect security classified resources. These traits include honesty, trustworthiness, maturity, tolerance, resilience and loyalty.

92. **Procedural Fairness**. An administrative law principle that ensures a fair and proper procedure is followed when making a decision.

93. **Security Officer.** A role occupied by an individual in an Industry Entity with delegated authority from the Chief Security Officer to undertake the day-to-day management of protective security.

94. **Suitability**. Criteria outlining an Industry Entity's ability to demonstrate they can meet suitability requirements for DISP membership, outlined in the DISP Suitability section of DSPF Control 16.1.

Annexes

Annex A – Defence Industry Security Program – DISP Membership Level Requirements

Annex B – Defence Industry Security Program – Contacts and

Resources

Document Administration

Identification

Control	Defence Industry Security Program
Control Owner	Assistant Secretary Defence Industry Security
Control Version	10
Publication date	29 January 2026
Releasable to	Defence, Defence Industry, and Public
Underlying DSPF Principles	Personnel Security Clearance Temporary Access Classification and Protection of Official Information Systems Security Cyber Security Assessment and Authorisation 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
4	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
5	17 February 2022	AS SPS	Rewritten policy to improve the uplift of industry security and engagement
6	1 August 2022	AS SPS	Update to Escalation Threshold table, DRICS reference, workplace standard, and Entry Level and Level 3 membership requirements
7	30 March 2023	AS SPS	Update Paragraph 21 clarifying email address requirements for DISP members/applicants.
8	24 November 2023	FAS DS	Transfer of Control Ownership from AS SPS to AS DIS
9	27 September 2024	AS DIS	Refresh text to reference the Defence Industry Security Branch and the DISP Member Portal; update mandatory membership provisions; clarify CSO and SO PSC requirements; upgrade cyber security requirements; include Special Access Programs Annex.
10	29 January 2026	AS DIS	Updated ‘releasable to’

Defence Security Principles Framework (DSPF)

Annex A to Defence Industry Security Program – DISP Membership Level Requirements

Conditions applicable to all Industry Entities

1. All Industry Entities must:

   a. meet and maintain the requirements outlined in Control 16.1 – Defence Industry Security Program (DISP);

   b. demonstrate they have met, and are able to maintain, the requirements described in this Annex;

   c. ensure the Security Governance domain matches or exceeds the highest level of membership sought for any other domain; and

   d. engage with audit and uplift activities conducted by Defence (or a third party nominated by Defence).

2. Defence may refuse, downgrade, limit, suspend or terminate DISP membership if:

   a. the eligibility and suitability criteria have not been met, or are no longer being met; and/or

   b. it is determined that granting or continuing an Industry Entity's DISP membership is not in the national or Defence's interest.

Note: *The Defence Industry Security Branch (DISB) is available to assist Entities to determine their eligibility requirements and cyber security standards.*

Membership Level Requirements

Membership Categories	Security Governance	Personnel Security	Physical Security	Information and Cyber Security
Entry Level 	Entities **must**: • appoint and retain a Chief Security Officer (CSO) and at least one Security Officer (SO). NB: the CSO and SO can be the same individual. • establish and maintain policies and procedures, inclusive of registers and reporting activity/incidents, covering: - security governance arrangements, including designated security positions and their contact details; - risk management, inclusive of security considerations and business security risk assessments; - security training arrangements for all personnel; - security incidents, inclusive of a register covering all security incidents across all security types i.e. personnel, physical, information and cyber incidents; - security reporting arrangements (including security incidents and contact reporting) and register of contacts with foreign persons and entities; - a register of overseas travel with completed travel forms and records of travel briefings provided to security cleared personnel; and - arrangements and training for insider threat identification, reporting and	Entities **must**: • establish and maintain policies and procedures in accordance with the Australian Workforce Screening Standard AS4811-2022. • Establish and maintain policies and procedures for: - on-boarding personnel; - ongoing assessmen t of personnel; and - separating personnel. • establish and maintain a register of Designated Security Assessed Positions (DSAP) of all personnel with security clearances within the Industry Entity, including job role/position and security clearance level. This register **must** be made available to Defence on request. • report the engagement of foreign nationals and any other disclosures that may be of interest to Defence. • provide Defence a copy of workforce screening and management	Entities **must**: • establish and maintain policies and procedures covering details of physical security and access controls at each accredited facility and their location. provide facility ownership and leasing arrangement details to Defence as required.	Entities **must**: • meet or exceed the Australian Signals Directorate's (ASD) Essential Eight (Essential 8) at Maturity Level 2 across all of the Entity's ICT corporate systems used to correspond with Defence. • Entities who comply with other international security standards can use their documentation to demonstrate in part how they meet the Essential 8. These standards include: - Information security management: ISO/IEC 27001:2022 - Protecting Controlled Unclassified Information in Non-Federal Systems and Organisations (US ITAR requirement): NIST SP 800 – 171 - Cyber security for Defence: Def Stan 5-138. These standards are not equivalent to the Essential 8. You will still need to demonstrate how you meet all Essential 8 mitigation strategies in the DISP Cyber Security Questionnaire. **Note**: If ASD's

	management. • engage in all annual DISP assurance activities, including, but not limited to: - annual DISP security reporting; - completing annual security training; and - implementing relevant uplift and assurance programs in accordance with agreed uplift and assurance requirements. • notify Defence of changes affecting membership, including changes to: - ownership, board memberships, and financial structures/control; - financial position and financial viability; - international supply chain activities; - exposure to criminal or other unlawful activities; and - any other activity or incident which may influence the Entity's ability to continue working with Defence. The Entity's nominated CSO and SO **must**: • complete the DISP Security Officer Training course as part of the application process, and every three years thereafter; and • be able to demonstrate the ability or have relevant experience to manage personnel/facilities and information and cyber security up to and including an 'OFFICIAL/ OFFICIAL: Sensitive' level. The Entity's nominated SO **may**: • request access to the DISP Security Portal to access security documents, templates, forms and tools relevant to performing their role.	processes of personnel working with or on Defence-related work. The Entity's nominated CSO and/or SO **must**: • be Australian citizens and be able to obtain and maintain a minimum Baseline security clearance, in accordance with the Australian Government Security Vetting Agency (AGSVA) policy. The SO cannot sponsor security clearances.		Essential 8 is superseded, the Information and Cyber Security requirements will be updated to align with the latest version.

Membership Categories	Security Governance	Personnel Security	Physical Security	Information and Cyber Security
Level 1	Entities **must**: • meet or exceed all security governance requirements in Entry Level. • establish and maintain a register of all personnel sponsored for a security clearance by the Entity • complete all annual assurance activities. The Entity's nominated SO **must**: • maintain a NV1 clearance. • be able to demonstrate the ability or have relevant experience to manage personnel/facilities and information and cyber security up to and including 'PROTECTED' level.	Entities **must**: • meet or exceed all personnel security requirements in Entry Level. • complete all annual assurance activities. The Entity's nominated SO **must**: • complete assurance activities required to maintain an NV1 security clearance. • be able to provide active monitoring and management of the ongoing suitability of sponsored security cleared personnel, including the monitoring of attitudes to security and behaviours in accordance with AGSVA policy. For the purpose of sponsoring personnel security clearances within their Industry Entity commensurate to their membership level, the Entity's nominated SO **must** be able to obtain and maintain a Negative Vetting level 1 security clearance. The SO is eligible to sponsor security	Entities **must**: • meet or exceed all physical security requireme nts in Entry Level. • ensure at least one facility is certified and accredited in accordance with the DSPF Principle 72 and Control 72.1 Physical Security to receive, handle, store and destroy 'PROTECTED' information and material in accordance with the ISM/ DSPF. • provide facility ownership and leasing arrangement details to Defence as required.	Entities **must**: • meet or exceed all information and cyber security requirements in Entry Level. • ensure at least one system is certified and accredited in accordance with the DSPF Principle 23 and Control 23.1 Cyber Security Assessment and Authorisation to receive, handle, store and destroy 'PROTECTED' information and material in accordance with the ISM/DSPF. • maintain the required physical security zoning where system servers are located.

		clearances up to and including the Baseline level.		

Membership Categories	Security Governance	Personnel Security	Physical Security	Information and Cyber Security
Level 2	Entities **must**: • meet or exceed all security governance requirements in Level 1. Entities are recommended to: • have arrangements agreed between the Entity and sponsoring the Commonwealth Government entity for the management of compartment briefs by a Defence Communications Intelligence Security Officer (COMSO). The Entity's nominated SO **must**: • be able to demonstrate the ability or have relevant experience to manage personnel/facilities and Information and cyber security up to and including 'SECRET' level.	Entities **must**: • meet or exceed all personnel security requirements in Level 1. The SO is eligible to sponsor security clearances up to and including the NV1 level.	Entities **must**: • meet or exceed all physical security requirements in Level 1. • ensure at least one facility is accredited in accordance with the DSPF Principle 72 and Control 72.1 Physical Security to receive, handle, store and destroy 'SECRET' information and material in accordance with the ISM/DSPF. • provide facility ownership and leasing arrangement details to Defence as required.	Entities **must**: • meet or exceed all information and cyber security requirements in Level 1. • ensure at least one network is accredited in accordance with the DSPF Principle 23 and Control 23.1 Cyber Security Assessment and Authorisation to receive, handle, store and destroy 'SECRET' information and material in accordance with the ISM/DSPF. • maintain the required physical security zoning where system servers are located.

Membership Categories	Security Governance	Personnel Security	Physical Security	Information and Cyber Security
Level 3	Entities **must**: • meet or exceed all security governance requirements in Level 2. • have documented and agreed endorsement from a Commonwealth Government Senior Executive Service Band 3, or equivalent Australian Defence Force (ADF) position, before: - obtaining a Positive Vetting clearance; and/or - the certification and accreditation of a Secure Compartment Information Facility (SCIF) and/or a 'TOP SECRET' network. • have arrangements agreed between the Entity and the sponsoring Commonwealth Government entity for the management of compartment briefs by a Defence Communications Intelligence Security Officer (COMSO). The Entity's nominated SO **must**: • be able to demonstrate the ability or have relevant experience to manage personnel/facilities, and Information and cyber security up to and including 'TOP SECRET' level.	Entities **must**: • meet or exceed all personnel security requirements in Level 2. The Entity's nominated SO **must**: • complete annual assurance activities required to maintain a Negative Vetting 2 (NV2) security clearance. • ensure compartment holders adhere to compartment requirements in accordance with the agreed sponsoring Commonwealth Government entity arrangements. The SO is eligible to sponsor security clearances up to and including the NV2 level.	Entities **must**: • meet or exceed all physical security requirements in Level 2. • ensure at least one facility is certified and accredited in accordance with the DSPF Principle 72 and Control 72.1 Physical Security to receive, handle, store and destroy 'TOP SECRET' information and material in accordance with the ISM/DSPF. • provide facility ownership and leasing arrangement details to Defence as required.	Entities **must**: • meet or exceed all information and cyber security requirements in Level 2. • ensure at least one network is certified and accredited in accordance with the DSPF Principle 23 and Control 23.1 Cyber Security Assessment and Authorisation to receive, handle, store and destroy 'TOP SECRET' information and material in accordance with the ISM/DSPF. • maintain the required physical security zoning where system servers are located.

Relevant DSPF Controls

Security Governance	Personnel Security	Physical Security	Information and Cyber Security
DSPF Governance and Executive Guidance	Principle 22 – Information and Technology Security (Personnel)	Principle 21 – Information and Technology Security (Physical)	Principle 10 – Classification and Protection of Official Information
	Principle 40 – Personnel Security Clearance	Principle 71 – Physical Transfer of Official Information, Security Protected and Classified Assets	Principle 15 – Foreign Release of Official Information
	Principle 41 – Temporary Access to Classified Information and Assets	Principle 72 – Physical Security	Principle 20 – Information and Technology Security (Log Management)
		Principle 73 – Physical Security Certification and Accreditation	Principle 23 – Cyber Security Assessment and Authorisation
		Principle 74 – Access Control	Principle 27 - Information and Technology Security (System Planning, Procurement and Supply Chain)
			Principle 28 - Information and Technology Security (System Management)

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document Administration

Identification

Annex	Defence Industry Security Program – DISP Membership Requirements
Annex Version	7
Annex Publication Date	29 January 2026
Releasable to	Defence, Defence Industry and Public
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 Principle	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
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	17 February 2022	AS SPS	Replacement of previous Annex A - Privacy Notice
4	4 March 2022	AS SPS	Update to clarify clearance sponsorship eligibility for each DISP level
5	1 August 2022	AS SPS	Update to workplace standard, and Entry Level and Level 3 membership requirements
6	27 September 2024	AS DIS	Update references and change minimum cyber security standards.
7	29 January 2026	AS DIS	Updated ‘releasable to’ and relevant DSPF Control references

Defence Security Principles Framework (DSPF)

Annex B to Defence Industry Security Program – Contacts and Resources

DISP Contacts

DISP general enquiries	1800 DEFENCE (1800 333 362)
DISP application enquiries and membership changes	DISP.info@defence.gov.au
Security Reporting • Security Incidents • Contact Reporting	security.incidentcentre@defence.gov.au

Resources

DISP website	DISP website
DISP Member Portal	DISP Member Portal
Defence Industry Security Program Application (AE250) for **upgrades only**	DISP Application (AE250)
Foreign Ownership Control and Influence (AE250-1) for **upgrades only**	FOCI (AE250-1)
Notification of Engagement requiring DISP Membership Portal	Notification of Engagement Requiring DISP Membership Portal

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document Administration

Identification

Annex	Contacts and Resources
Annex Version	5
Annex Publication Date	29 January 2026
Releasable to	Defence, Defence Industry and Public
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 Principle	16

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
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	17 February 2022	AS SPS	Replacement of previous Annex B – Suitability Matrix
4	27 September 2024	AS DIS	Update of links and contacts.
5	29 January 2026	AS DIS	Updated ‘releasable to’

Australian Government
Defence

Defence Security Principles Framework (DSPF)

Annex C to Defence Industry Security Program – Special Access Program

Special Access Program

1. Defence applies security procedures and practices, supported by legally binding obligations, to protect classified information. International agreements detail arrangements to protect classified information received from other nations. Some sensitive capabilities and activities require enhanced protection measures beyond those normally applied to information classified as SECRET or TOP SECRET.

2. The Defence Special Access Program (SAP) is a program established for a specific class of information that imposes safeguarding and access requirements – additional security controls – that exceed those normally required for information at the same classification level. Capabilities protected by a SAP include sovereign-developed capabilities and capabilities shared by Australia's partner nations.

Industry Participation in SAP

3. Industry Entities participating in SAP and/or accessing SAP information **must**, at a minimum, hold Defence Industry Security Program (DISP) Level 3 membership in the Governance and Personnel Security domains.

4. Special Access Program Policy provides a principles based, outcomes focused framework for SAP management. The SAP policy is supported by a SAP Framework which provides procedural guidance on the management, administration, operation and security of SAP by Defence Officials and industry. The SAP Framework should be read in conjunction with this Annex.

5. Industry Entities **must** agree to and apply the security controls outlined in SAP Framework, in addition to their obligations as DISP members, and be able to demonstrate they have implemented those minimum compliance standards.

6. The Defence Chief Security Officer (CSO) may, in consultation with the SAP Control Officer (SAPCO), make ongoing participation of a DISP member in SAP subject to additional security measures. The CSO will communicate such additional requirements to the DISP member in writing.

Industry Obligations

7. Industry Entities participating in SAP **must**:

   a. continue to apply all normal and enhanced protection measures.

   b. apply all additional security measures as and when required by the CSO.

   c. maintain records of security measures applied.

   d. submit to governance and assurance measures including, but not limited to, no-notice compliance audits as required by SAP Framework, and/or at the discretion of the CSO.

Non-compliance

8. Where an Industry Entity fails to comply with their obligations under this Annex, the CSO may limit, downgrade, suspend or terminate an Industry Entity's DISP membership, in consultation with SAPCO and the relevant contract manager (or capability manager). Access to SAP is at the discretion of SAPCO.

9. The DISP membership suspension and termination provisions detailed in DSPF Control 16.1 paragraphs 44-46 will apply to identified non-compliance or security control breaches.

Key Definitions

10. **Special Access Program (SAP).** The Special Access Program is a set of enhanced security measures protecting information considered vital to preserving the military advantage of a Defence capability, plan or concept, where standard protective controls and procedures are deemed insufficient.

11. **SAP Framework.** The SAP Framework provides Australian policy on the management, administration, operations and security of Special Access Programs by the Australian Department of Defence.

12. **SAP Access Approval Authority.** Director General Special Access Program is appointed the Access Approval Authority (AAA) for Australian SAP or for a partner SAP where AAA has been delegated to an Australian official.

13. **Special Access Program Branch.** SAP Branch (SAPB) is the national office supporting the Vice Chief of the Defence Force as Accountable Officer for SAP. SAPB is the point of contact for enquiries on policy, access control, certification and accreditation requirements.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document Administration

Identification

Annex	Special Access Program
Annex Version	2
Annex Publication Date	29 January 2026
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 Principle	16

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	27 September 2024	AS DIS	Launch
2	29 January 2026	AS DIS	Updated references and links to SAP Framework

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 classified information and assets requires individuals to have an appropriate clearance and 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 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 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. Approval for access to ICT networks involving SIGNIFICANT and HIGH risks are to be implemented by Assistant Secretary Defence Cyber Information and Assurance Branch (ASDCIA) in the Joint Capabilities Group (JCG) as the Control Implementer.

10. Any misuse of temporary access provisions is reported as a security incident.

Escalation Thresholds

Risk Rating	Responsibility	
Low	Defence personnel in consultation with their Supervisor, Commander, or Manager	
Moderate	EL2/0-6 or equivalent in relevant Group/Service	
Significant	AS SPS	ASDCIA for ICT systems access only
High	Defence Security Committee (DSC) – through AS SPS	ASDCIA for ICT systems access only
Extreme	DSC through AS SPS	

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

Document administration

Identification

DSPF Principle	Temporary Access to Classified Information and Assets
Principle Owner	First Assistant Secretary Defence Security Division (FAS DS Division)
DSPF Number	Principle 41
Version	3
Publication date	31 July 2020
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 Government physical security management protocol Australian Security Intelligence Organisation (ASIO), Security Equipment Guides (SEGs) are available on the Defence Security Guidance Tools and Templates intranet page 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	12 August 2019	AS SPS	To reflect the appointment of ASICTS as Control Implementer for Significant and High risk ICT systems access.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy

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.

Control Implementer

2. AS SPS has formally designated Assistant Secretary Defence Cyber Information and Assurance Branch (ASDCIA) in the Joint Capabilities Group (JCG) as the Control Implementer for ICT systems access for SIGNIFICANT and HIGH risk. ASDCIA will manage all approvals for temporary access to ICT systems in accordance with the Escalation Thresholds below.

Escalation Thresholds

3. 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	ASDCIA for ICT systems access
High	Defence Security Committee (DSC) – through AS SPS	ASDCIA for ICT systems access
Extreme	DSC through AS SPS	

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

Controls

Temporary Access

4. 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 classified information and assets accessed under these arrangements.

Note: *For the purposes of this Control, 'classified information' refers to PROTECTED or higher.*

5. Temporary access is to be strictly confined to the specific 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.

6. Temporary access is not a security clearance and **must not** be used in lieu of a security clearance to provide assurance for reasons other than access to specific 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.*

Note: *Defence policy mandates that Defence personnel hold a minimum security clearance of Negative Vetting 1 (NV1) prior to having independent access to bulk weapons. Temporary access cannot be used to satisfy this requirement.*

Note: *Temporary access is not a security clearance and therefore cannot be used to allow unescorted access to Security Zones Three, Four and Five.*

Temporary Access, Caveats, DLM and Need-to-Know

7. 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.

8. 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 and Compartmented information.*

Example: *An Australian Defence Force member has a current Negative Vetting 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

9. 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 Release 2024: *17 Access to Resources.*

Requirements and Constraints on Temporary Access

10. 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. See PSPF Release 2024: *17 Access to Resources.*

11. In addition to limitations applied within PSPF Release 2024: *17 Access to Resources*, Temporary access:

a. **must not** be approved:

(1) to permit access to any material classified TS unless the person requiring the access holds an Australian Government Negative Vetting Level 1 clearance;

(2) retrospectively to avoid managing a security incident resulting from unauthorised or incidental access to classified material; or

(3) 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:

(1) by Defence personnel. Defence Industry cannot approve Temporary access on behalf of the Australian Government; and

(2) if the scope of the approved information access can be defined and the ownership of the information is understood.

12. Temporary access is only available to persons who either currently hold, or are eligible to be considered for an Australian Government security clearance.

13. 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.*

14. 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).

ICT Systems Access

15. The approval of Temporary access does not permit unrestricted access to Defence ICT networks. If Temporary access is required for 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 appropriately cleared system user.

16. Normal user access on systems such as the Defence Protected Network (DPN) and Defence Secret Network (DSN) grant access to large volumes of information on websites 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.

17. ASDCIA is the Control Implementer for ICT systems access requests involving SIGNIFICANT and HIGH risk. Therefore, requests for access involving these risk thresholds are required to be made to ictsec.advice@defence.gov.au for approval.

a. JCG mandates that 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

18. For information regarding the granting of Temporary access to MOPS Act staff, see PSPF Release 2024: *20.3 Members of Parliament (Staff) Act Employees*.

19. 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 1/07 (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)	Minimum of SES Band 1/07 (or approved delegate) in consultation with AGSVA SADFO (only for SAFEBASE related emergencies)

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 Release 2024: *20.3 Members of Parliament (Staff) Act Employees*).

Note: *Chief Joint Operations (CJOPS) discharges these responsibilities in respect of personnel on overseas operations.*

Processing Temporary Access Requests

20. The area approving Temporary access **must** 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 Release 2024: *17 Access to Resources.*

21. The Commander or Manager (or their delegate) of the area seeking Temporary access for an employee **must**:

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 via an SVA-046 *Temporary Access to Classified Resources* form;

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 e. 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:

   (1) upgrade the position's security clearance requirement; and

   (2) initiate a security clearance upgrade for the individual.

Note: *Contract Managers discharge these responsibilities in respect of the persons engaged under a contract that they manage.*

22. 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 access.

Temporary Access Denied

23. Temporary access decisions are not final security clearance decisions as they are based on incomplete information that does not allow for a full assessment of the whole person. Therefore a 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 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

24. **Australian Government Security Vetting Agency**: AGSVA is a branch of the Defence Security Division (DS) that provides independent security clearance vetting services and advice to non-exempt government agencies (including Defence).

25. **MOPS Act staff**: Staff employed by an Australian Government Minister under the *Members of Parliament (Staff) Act 1984 (Cth)*.

26. **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 need-to-know.

27. **Temporary access**: A temporary arrangement that in some 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.

28. **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.

29. **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.

30. **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.

31. **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

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

33. 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
Control Implementer	Assistant Secretary Defence Cyber Information and Assurance Branch
DSPF Number	Control 41.1
Version	5
Publication date	27 March 2025
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	12 August 2019	AS SPS	To reflect the appointment of ASICTS as Control Implementer for Significant and High risk ICT systems access.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	13 January 2025	FAS DS	Amended outdated positions, strengthened requirements, and aligned to Physical Security Zone changes.
5	27 March 2025	AS SPS	Amended terminology referring to security clearance requirements for Physical Security Zone access.

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. International travel may expose Defence personnel and persons engaged under a contract to threats which could compromise national security and personal safety. Such threats may not be present in Australia and may therefore not be anticipated by travellers. For this reason it is crucial that travellers are briefed before travel to raise awareness of their destinations security environment, to ensure that adequate precautions are taken.

Expected outcomes

3. Defence personnel and persons engaged under a contract: **are expected to**:

a. notify relevant departmental authorities of their travel plans in a timely manner;

b. be aware of security risks relevant to their travel destination;

c. be aware of additional security risks they may expect if they are a Sensitive Compartmented Information access holder;

d. protect official information (if being carried or accessed for official travel);

e. report suspicious contacts, security incidents or security concerns to their Security Officer (SO) and Defence Security via submission of an XP188 (Security Report), and the Australian Signals Directorate if a member of a Defence Intelligence Agency);

f. ensure that official visits to allied facilities are conducted in accordance with bilateral security responsibilities and hosting country business processes;

g. use their official Australian passport to exit and return to Australia if they are holders of a Positive Vetting clearance (unless granted specific permission to do otherwise) and travelling for official purposes; and

h. remain aware of their security responsibilities (as per the DSPF) during travel.

Note: *Certain countries, including the United States of America and Canada, have moratoriums and minimum lead times for processing official travel visit requirements. The Australian Government Security Vetting Agency (AGSVA) can be contacted for further advice regarding request for visits.*

4. Defence personnel and persons engaged under a contract are not to make false declarations regarding their employment. If required, the traveller is to list their status as 'government employee' or 'contractor'.

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

Document administration

Identification

DSPF Principle	Overseas Travel
Principle Owner	First Assistant Secretary Defence Security (FAS DS)
DSPF Number	Principle 44
Version	4
Publication date	13 January 2025
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 website Security forms and tools available on the Defence Security Services intranet page: 1. Overseas Travel Briefing and Debriefing (Web form AB644) 2. DSN country-specific threat advice 3. Security of Information Agreements and Arrangements (SIAs) 4. Defence Security and Counterintelligence

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	August 2019	FAS S&VS	See DSPF Amendment List 1
3	30 May 2020	FAS S&VS	Deletion of references to DFAT Smartraveller registration and DSM and minor grammar updates
4	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
5	13 January 2025	FAS DS	Passport terminology clarification provided, and other minor updates.

Australian Government
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

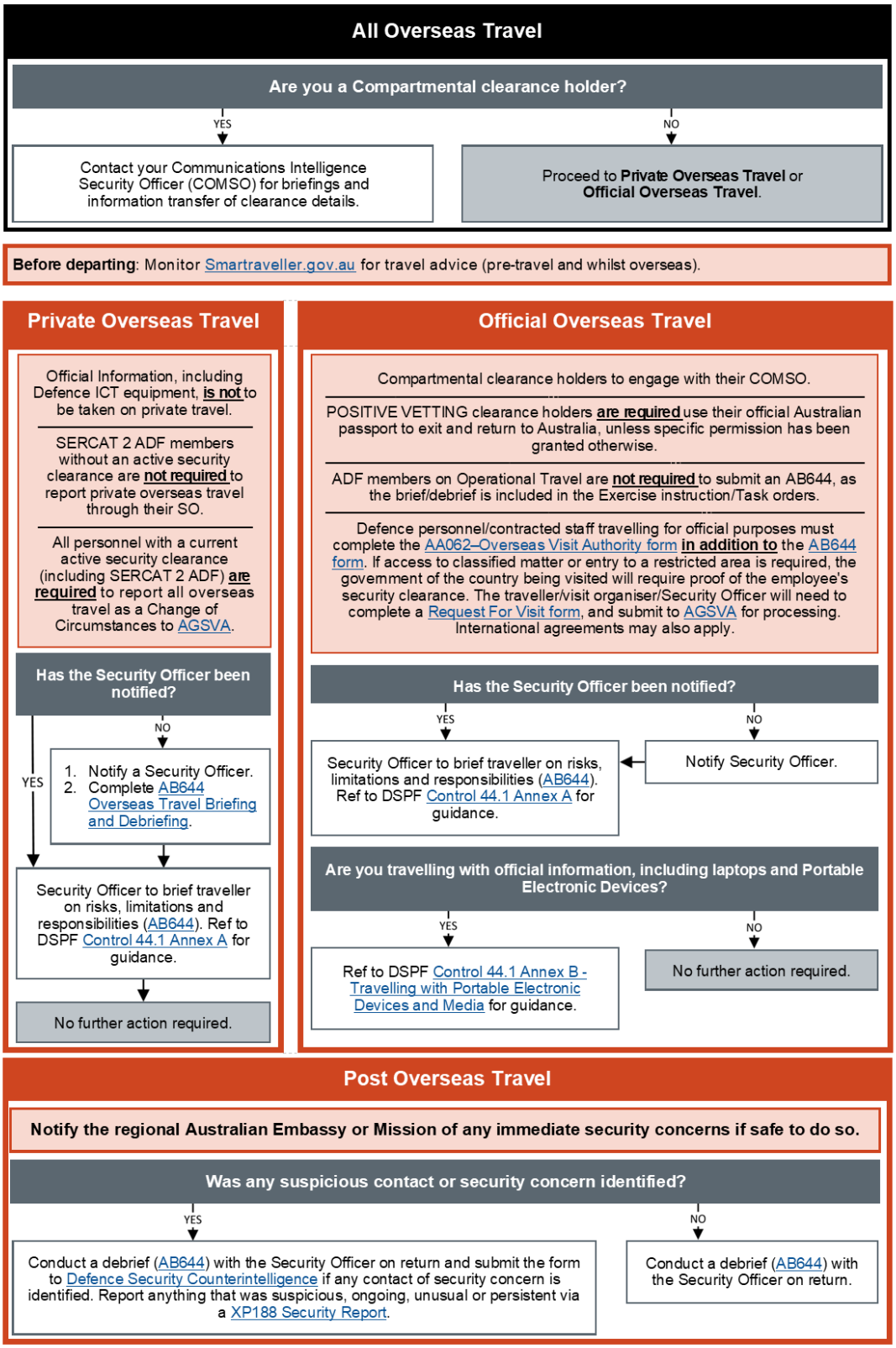
2. AS SPS has set the following general thresholds for risks managed against this Defence Security Principles Framework (DSPF) Control, and related Principle and Expected Outcome.

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

3. Figure 1 outlines the Overseas Travel security process.

Figure 1: Overseas Travel Security Process



Roles and Responsibilities

Defence Security Division Visits team, Australian Signals Directorate, Group and Service Executive Security Advisers

4. The Defence Security Division (DS Division) Visits team, Australian Signals Directorate (ASD) Security and Integrity, and the Group and Service Executive Security Advisers (ESAs) are responsible for providing overseas security travel advice and monitoring compliance requirements.

5. The DS Division Visits team is responsible for end-to-end security clearance processing, including referring the clearance details of Defence personnel and persons engaged under a contract to foreign governments, and confirming foreign national security clearance details in accordance with Security of Information Agreements and Arrangements (SIA).

6. ASD Security and Integrity is the compartment sponsor of Defence personnel and persons engaged under a contract and is responsible for notifying a foreign government of the details (if held) of a traveller's Sensitive Information Compartments (SIC).

All Defence personnel

7. All Defence personnel (APS employees [including SERCAT 1] and ADF members [all SERCATs]) **must** report all Defence official overseas travel through their Security Officer (SO), via an AB644 – Overseas Travel Briefing and Debriefing form.

8. All Defence personnel (APS employees [including SERCAT 1] and ADF members [SERCATs 3 to 7]) **must** report all personal overseas travel through their Security Officer (SO), via an AB644 – Overseas Travel Briefing and Debriefing form.

9. SERCAT 3, 4 and 5 members who travel overseas in their civilian employment must also report this through their SO. SERCAT 2 ADF members are not required to report personal overseas travel through their SO.

10. All Defence personnel (APS employees [including SERCAT 1] and ADF members [SERCAT 2 to 7]) with a current active security clearance **must** report all overseas travel as a Change of Circumstances to AGSVA via the myClearance portal, in addition to reporting requirements required by Defence.

11. Submit required forms (AA062 and AB644, as well as an XP090 if required) for official travel.

12. Submit a 'Log a Job Online' if intending to take Defence ICT mobile devices for official travel.

13. If compartmentally briefed, report to their relevant compartment controller prior to overseas travel.

Commanders and Managers

14. Commanders and Managers are responsible for processing and approving overseas travel requests and for ensuring that all Defence personnel and persons engaged under a contract travelling overseas are aware of their security responsibilities in accordance with the DSPF.

Security Officers

15. The Security Officer (SO) is responsible for necessary administrative action to ensure compliance with the DSPF on behalf of their Commander, Manager or Defence Industry Security Program member executive. Mandatory administrative actions include:

a. recording travel details from the AA062 Overseas Visit Authority form (for official overseas travel) and the AB644 – Overseas Travel Briefing and Debriefing (for private travel) in the Security Register and maintaining a copy of the forms at unit level. Where Defence/industry personnel are required to carry a Defence-issued Mobile ICT device, the SO is to confirm and note on the AB644 the details of the approval prior to departure, and confirm and record the details of the 'notification of return' during the post-travel security debrief.

   Note: Defence personnel undertaking official overseas travel **must** complete **both** the AA062 and the AB644 forms.

   Those undertaking private travel **must** complete the AB644.

b. supporting Defence personnel and persons engaged under a contract in complying with their security responsibilities in accordance with the DSPF, including assisting compartmentally-briefed personnel report intended travel to the relevant compartment controller via ASD Security and Integrity or their Communications Intelligence Security Officer (COMSO);

c. providing overseas travel briefings and debriefings (within 30 days of the traveller's return), including following up as required anything noted in the completed post travel - Section 4 – Debrief in AB644 – Overseas Travel Briefing and Debriefing;

d. ensuring that all ICT requirements on the Overseas travel and visits page have been considered and actioned accordingly (see Annex B to this Control for further information);

e. confirming that (if required) a Request for Visit or XP090 Overseas Request for Visit or Posting Security Clearance Advice (depending on the nation being visited) has been completed for official travel and sent to the DS Division Visits team via securityclearances@defence.gov.au within the required timeframe specified in the SIA.

f. Ensure any personnel that are holders of a Positive Vetting (PV) clearance have been informed that they **must** use their official Australian passport to exit and return to Australia when travelling for official purposes (unless granted specific permission to do otherwise). PV holders are to seek approval to travel to certain countries, as stated in the Sensitive Material Security Management Protocol (within the Protective Security Policy Framework).

16. In the absence of an SO, the Commander or Manager is to allocate an alternate SO to conduct the overseas briefings and debriefings.

Example: *If a traveller with a Negative Vetting 1 clearance, and no Sensitive Compartment Information brief has no SO available for the travel brief or debrief, the unit COMSO is a suitable alternate.*

Types of Defence travel

17. There are three distinct categories of Defence travel; Private, Official and Operational.

18. Submission of an AB644 Overseas Travel Briefing and Debriefing form is not required for Operational travel for ADF members, as this briefing/debriefing is included in Exercise instruction/Task orders as required.

Key Definitions

Further Definitions

19. 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	7
Publication date	17 February 2026
Type of control	Enterprise
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 Information and Technology Security (Personnel) Information and Technology Security (Portable Devices and Media) 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
2	30 May 2020	AS SPS	Deletion of references to DFAT Smartraveller registration, minor grammar, removal of duplicated information and references to the DSM
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	18 October 2023	AD ESP	Administrative update to align with new form and organisational names.
5	13 January 2025	FAS DS	Additional mandatory provisions and explanatory ICT information included, AB644/AA062 forms clarification provided, and Figure 1 Overseas Travel Security Process map updated.
6	13 May 2025	FAS DS	Service Category (SERCAT) travel reporting requirement guidance revised.
7	17 February 2026	AS SPS	Figure 1: Overseas Travel Security Process updated.

Australian Government
Defence

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 overseas travel.

2. **Note**: the AA062 - Overseas Visit Authority and the AB644 - Overseas Travel Briefing and Debriefing are to be completed for official travel. Those undertaking personal travel are only required to complete the AB644.

Table 1: Briefing Process Prior to Overseas Travel

Stage	Who does it	Description
1	Traveller	**For official travel**: Complete the AB644 – Overseas Travel Briefing and Debriefing form and the AA062 - Overseas Visit Authority for official travel form. The traveller will also need to complete a Request For Visit form, or (depending on the nation being visited, the XP090 Overseas Request for Visit or Posting Security Clearance Advice) and submit to AGSVA for processing. **For private travel**: Complete the AB644 form. (Note: Control 44.1 provides a comprehensive breakdown on travel reporting requirements for each Service category [SERCAT] Send relevant form to their Security Officer as soon as they plan to travel. Contact your Communications Intelligence Security Officer (COMSO) for specific compartmented briefings (if applicable).
2	Security Officer	Conduct an overseas travel briefing with the person travelling. Complete the pre-travel Security Officer section of the AB644 form. Confirm that the person travelling has had required compartment briefings.
3	Traveller	Obtain 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	Record travel details in the Security Register. Retain the completed AB644 and/or AA062 forms Consideration should be given to whether the traveller: 1) the person travelling has a high level of access; 2) DFAT has issued a Consular Travel Advisory Notice or Bulletin for countries being visited or transited through; or 3) the person is travelling with a Defence-issued or Defence Industry Security Program laptop or Portable Electronic Device (PED), and is not protected by a *Laissez-Passer* (refer Definitions below).
5	Security Officer and Traveller	If there are any contact or security concerns, the Security Officer or the traveller are required to submit an XP188 Security Report with attached AB644 form or AA062. All security clearance holders are to report any overseas travel as a Change of Circumstances to AGSVA via the myClearance portal.

Debriefings

3. The table below outlines the process for debriefing a traveller returning from overseas.

Table 1 – Debriefing Process When Returning from Overseas

Stage	Who does it	Description
1	Traveller	Complete the debriefing section of the AB644 with their Security Officer.
2	Security Officer	Conduct an initial debriefing using the debriefing section of the AB644.
3	Traveller	Complete and submit relevant online forms (if applicable) to report any suspicious approach, event, or action (whether deliberate, reckless, negligent, or accidental) via a: • XP188 – Defence Security Report.
4	Security Officer	Retain copies of completed forms (AB644 and XP188) at Unit/Facility level.

Issues Covered in Debriefings

4. Travel debriefing is a formal process to discuss events that occurred during the visit, and to identify events which could later be used to threaten the security of the individual. This is a discussion not an interrogation, and the returning traveller should not be questioned as such.

5. Debriefing discussions include:

6. Travel procedures:

a. **Visa** – How and by whom the visa was obtained? Were any probing questions asked about employment?

b. **Entry and exit procedures** – What occurred? Did officers/officials conduct any searches? Were documents examined out of sight? Was there any suspicious or concerning 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 directed to the traveller or to other members of the organised party?

7. Accommodation:

a. Where did the traveller stay?

b. How and by whom was the accommodation arranged?

c. Was there a choice in accommodation?

d. Did any hospitality staff appear to behave in an unusual manner? and

e. Were any occurrences of eavesdropping or searches of luggage or rooms observed?

(1) Was the traveller carrying official information or Defence-issued ICT or mobile devices (as defined in Annex B to Control 44.1)?

(2) Was the official information appropriately stored and/or accompanied?

(3) Was the official information left unattended in the traveller's hotel room at any time during the stay? and;

(4) Was the traveller's room cleaned or serviced while the traveller was absent?

8. Contact with local nationals:

a. Was any approach made to the traveller for any of the following reasons or did any of the following occur:

(1) currency exchange;

(2) bartering, such as an offer to purchase or swap any of the travellers belongings;

(3) sexual soliciting; or

(4) requests to carry mail/packages?

b. Was any excessive interest taken in the traveller's employment?

c. Was there any unusual contact with any uniformed official?

d. Drugs or suspected food/drink spiking?

e. Did anyone propose continued contact post visit? and

f. Were any invitations of any type extended?

Note: *This is not a definitive list of questions to ask, or reasons local nationals may seek to make contact with travelling Defence personnel and persons engaged under a contract*

9. Contact with other travellers or non-locals living in the country:

a. Was there any contact with tourists who did not seem to be genuine (e.g. people in their tour group, other hotel guests, other attraction visitors etc.)?

Definitions

10. ***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. The Laissez-Passer does not confer diplomatic immunity on personal hand luggage or other belongings. The Laissez-Passer and diplomatic pouch are issued to an individual and they 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	6
Annex Publication date	13 May 2025
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
2	30 May 2020	AS SPS	Minor grammar and content changes
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	12 May 2023	AS SPS	Form link corrections; Defence logo updated; minor addition to *Contact with local nationals* section; inclusion of reference to Control 30.1.
5	13 January 2025	FAS DS	Forms clarification (AB644/AA062, clarification regarding XP090/Request for Visit, removal of reference to Control 30.1, updated links.
6	13 May 2025	FAS DS	Minor updates to ensure terminology is aligned, and other minor updates.

Australian Government
Defence

Defence Security Principles Framework (DSPF)

Annex B to Overseas Travel – Travelling with Defence Issued Mobile ICT Devices

Travelling Overseas with a 'Handle As' Classification of OFFICIAL

1. When Defence personnel and persons engaged under a contract travel overseas on Defence business with Defence mobile ICT devices, including removable media with an actual Protective Marking of OFFICIAL, OFFICIAL: Sensitive (O: S) or PROTECTED, Defence mobile ICT devices are to be encrypted with an Australian Signals Directorate (ASD)-approved product accredited to reduce the 'handle as' classification to OFFICIAL, and carried as hand luggage.

2. Approval for carriage of Defence mobile ICT devices **must** be obtained from Joint Capability Group (JCG) via Log a Job Online (Defence Mobile ICT Devices - Request Overseas Use) prior to overseas travel for official Defence business purposes.

3. This **must** be done prior to going overseas as some configuration amendments that need to be made cannot be applied once the devices are overseas.

4. The carriage of Defence mobile ICT Devices will only be approved for Official Travel, Defence personnel are not permitted to take Defence ICT PEDs on overseas Private/Personal travel.

5. Where Defence/Industry personnel are required to carry a Defence issued mobile ICT device overseas, the Security Officer is to confirm and note on the AB644 the details of the approval prior to departure and confirm and record the details of the 'notification of return' during the post-travel security debrief.

6. Defence mobile ICT Devices include:

a. DREAMS Token/app or DCAC Reader for DREAMS

b. Protected iOS device (iPhone or iPad)

c. Defence Protected Laptop (DPL)

d. Official Phone/iPhone

e. Unclassified Laptop/Tablet/iPad (issued by Defence)

f. Defence-supplied SIM

g. Nighthawk

h. Burner devices (issued by Defence).

Travelling Overseas with an 'Actual' Classification of SECRET and Above

7. Defence mobile ICT devices, including removable media with a classification of SECRET, 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 mobile ICT device is encrypted with an ASD approved product to reduce its 'handle as' classification to OFFICIAL: Sensitive.

Storage Overseas

8. Physical access to a Defence mobile ICT device 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 mobile ICT device are reminded that they are not to store classified or sensitive material in hotel rooms or hotel safes unless that material, including the Defence mobile ICT device, 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 Mobile ICT device

9. Most countries equate the random search of a mobile device with a random luggage search. Defence personnel and persons engaged under a contract are not exempt from such searches and are to comply with the request for a search unless they are carrying a *Laissez-Passer* protecting the Defence mobile ICT devices.

Key Definitions

10. ***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	3
Annex Publication date	15 July 2024
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
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	15 July 2024	AS SPS	Updates made to overseas travel guidelines, processes, and mobility device information.

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 and persons engaged in contract 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 and persons engaged under contract 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 and persons engaged under contract 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 and persons engaged under contract are aware of the increased security risks associated with working offsite.

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 (or higher) in relevant Group/Service
High	Assistant Secretary Security Policy and Services (AS SPS)
Extreme	Defence Security Committee (DSC) – through AS SPS

Note: *Persons engaged under contract 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	2
Publication date	31 July 2020
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 ICT systems; Access to information; Entity physical resources; and Entity facilities. **Legislation:** *Work Health and Safety Act 2011* WHS Regulations WHS Codes 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)	Assessing and Protecting 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. PSPF – *15 Physical security for entity resources* (Working away from the office) 2. PSPF – *8 Sensitive and classified information* 3. PSPF – *5 Reporting on security* 4. Better Practice Checklist – 21. ICT Support for Telework 5. PSPF – *3 Security planning and risk management* 6. Defence People Group Telework Policy 7. Information Security 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	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy

Australian Government
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 (or higher) in relevant Group or Service
High	AS SPS
Extreme	Defence Security Committee (DSC) – through AS SPS

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

Introduction

3. Persons engaged under a contract undertaking approved offsite work within Australia, 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 working remotely 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 working remotely Policy.

Protecting Official Information

8. Defence personnel and persons engaged under contract are to ensure that Official Information is protected from unauthorised access. Refer to DSPF Principle 10 – *Assessing and Protecting Official Information*.

9. Defence personnel and persons engaged under contract **must not** allow people without the appropriate clearance, and a legitimate need-to-know, to access Official Information. The need-to-know principle applies at all times.

10. 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 OFFICIAL – in either hard copy or electronic (soft copy) format; and

b. Information that is OFFICIAL:Sensitive or 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 OFFICIAL:Sensitive 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.*

Hard Copy Documents

11. Approval in writing from a Commander, Manager or Contract Manager is required before Defence personnel and persons engaged under contract may remove OFFICIAL: Sensitive or higher (i.e. 'PROTECTED' and above) material from Defence premises to conduct offsite work.

a. Refer to DSPF Control 71.1 - *Physical Transfer of Information and Assets* and DSPF Control 72.1 - *Physical Security* for policy related to the authorised removal of this material

b. Refer to DSPF Controls 10.1 – *Assessing and Protecting Official Information* and 72.1 – *Physical Security* for policy related to the minimum physical storage requirements for Official Information.

12. An auditable record of protectively marked documents and material removed from Defence premises is to be maintained. Material classified TOP SECRET and above must be recorded in an XC-40 Classified Document Register (CDR) in accordance with Annex E to Control 10.1 –*Assessing and Protecting Official Information*.

13. Whilst in transit, Official 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 Control 71.1 - *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

14. Approval is required before Defence personnel and persons engaged under a contract may remove ICT equipment, or media with a 'handle as' classification of PROTECTED or above from Defence premises to conduct offsite work.

15. Encrypted ICT equipment or media with a 'handle as' classification may resume its actual classification once powered up, or when hibernating. Personnel **must** consider their environment and remain cognisant of their security obligations when using encrypted ICT equipment or media when working offsite. 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 OFFICIAL 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

16. 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.*

17. Offsite classified conversations are to be protected from being overheard or recorded. See PSPF *15 Physical Security for Entity Resources* – Working away from the office for guidance on the measures that can be used to reduce the threat of conversations being overheard or recorded.

18. Where classified conversations are conducted at home, e.g. on a secure phone, attention needs to be paid to the presence of uncleared persons.

Note: *Be mindful of your surroundings, such as children overhearing classified conversations. Exposing them to classified information is a security risk. Similar precautions should be taken with smart home devices, such as Google Home or Alexa. These devices should be turned off.*

19. Personnel **must not** continue with working offsite arrangements where there is an expectation that classified discussions occur regularly. Alternative working arrangements or expectations should be considered.

Note: *There is an increased risk of Foreign Intelligence Services (FIS) targeting premises where classified conversations occur regularly.*

Overnight Carriage

20. Overnight carriage of classified information is covered in DSPF Control 71.1 - *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

21. 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.

22. 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

23. Defence personnel and persons engaged under contract 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 Control 10.1 – *Assessing and Protecting Official Information*, DSPF Control 71.1 - *Physical Transfer of Information and Assets* and DSPF Control 72.1 - *Physical Security*.

24. 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.

25. 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 OFFICIAL. 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.*

26. If information or assets with a 'handle-as' or 'actual' classification of PROTECTED or above need to be stored at home, authorisation for offsite work is required from your commander/manager.

a. Refer to DSPF Control 71.1 – *Physical Transfer of Information and Assets* and DSPF Control 72.1 – *Physical Security* for policy related to the authorised removal and secure storage of the material.

Disposal of Official Information

27. Defence personnel and persons engaged under contract working offsite are required to dispose of classified waste in accordance with DSPF Principle 10 – *Assessing and Protecting 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

28. When Defence personnel and persons engaged under contract working offsite become aware of any incident that may indicate or suggest that 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*.

29. 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

30. 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 Control 22.1 – *Information and Technology Security (Personnel).*

Note: *The use of personal email accounts (such as Gmail, Hotmail and personal outlook accounts) and applications (such as Signal, Zoom and WhatsApp) cannot be used by personnel for the transmission or storage of Official Information, in accordance with Control 30.1 – Remote Access to Defence Systems. Refer to Control 10.1 – Assessing and Protecting Official Information for advice on protective markers and security classifications.*

31. Defence personnel and persons engaged under contract **must not** use privately owned devices to process or store any Defence Official Information that has not been authorised for public release, as per DSPF Control 22.1 – *Information and Technology Security (Personnel) .*

Exclusion: *In accordance with DEFGRAM 315/2020, the CISO and CSO have issued a dispensation to all of Defence until 30 October 2020 due to the COVID-19 pandemic. All Defence personnel, including persons engaged under contract, will be able to send and store OFFICIAL Information on privately owned devices.*

Example: *Alex is working from home using DREAMS. They are experiencing issues logging in to the DREAMS network and had a colleague forward Classified emails and documents to their Gmail account so they can continue working. This is a security breach.*

32. Defence Personnel and persons engaged under contract **must not** reclassify information in order to allow it to be sent, or accessed from, offsite. Reclassifications are only to occur in line with DSPF Control 10.1 – *Assessing and Protecting Official Information*.

Example: *Bob reclassifies a SECRET document to OFFICIAL in order to be able to access it remotely from home. This is a security breach and is not allowed.*

Offsite Work Approvals - Physical

33. Offsite work requiring the physical handling, storage or destruction of Official Information or an asset with a ‘handle-as’ classification of PROTECTED or above, other than CODEWORD information, requires the approval of (at minimum) an SES Band 1/O-7 in the user’s chain of command or the First Assistant Secretary Security and Vetting Service (FAS S&VS). This role cannot be delegated.

34. Approval from the originator **must** be provided when Defence is not the sole originator of the classified material.

35. 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/O-7, and additionally requires the prior approval of both ASIO and the originating agency.

36. The following questions are to be considered when approval for offsite work is being considered:

a. Has a current Security Risk Assessment (SRA) been completed?

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 Standard Operating Procedures (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 DSPF and any agreed SOPs?

37. Material is to remain in the personal custody of the individual and stored appropriately when not in use, in accordance with DSPF Control 72.1 - *Physical Security*.

Standard Operating Procedures (SOPs)

38. In addition to a formal agreement to undertake offsite work, it may be appropriate to develop SOPs – these may include:

a. specifying the highest classification of work to be conducted by the employee off site including:

(1) classification of discussions allowed;

(2) classification of information processed on ICT systems; and

(3) 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 requirement to report any security incidents at the premises to DSD;

j. procedures for the transfer of classified material between other Defence or approved premises and the home-based site; and

k. confirming the holder is prepared to accept responsibility for the safe custody of any material accessed while offsite.

Accreditation

39. For accreditation purposes, a home-based site is considered the same as any other Defence facility. Refer to the DSPF Control 73.1 - *Physical Security Certification and Accreditation* to determine if accreditation is required.

40. 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 (if using DREAMS), and the offsite device used to access the information is protected by an ASD-approved encryption that reduces the 'handle-as' classification to OFFICIAL or OFFICIAL: Sensitive when the device is not in use;

b. hard copies of information handled, stored or destroyed do not exceed the security classification of OFFICIAL.

Protecting Official Information at Events such as Conferences and Workshops

41. 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.

42. Security instructions should be developed before any event is held in a public venue or Zone One area involving security classified information, assets or other Official Information that has not been approved for public release.

43. 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 DSD); and

44. 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.

45. If classified information is to be discussed in non-accredited areas, advice **must** be obtained from either DSD, 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.

46. If classified information or assets need to be stored in a Zone One or Zone Two event site, for example overnight storage, advice should be obtained from the DSD regional office. Refer to DSPF Principle 72 - *Physical Security*.

47. For more general guidance on event security refer to *PSPF 15 Physical security for entity resources*.

Roles and Responsibilities

Deputy Secretary Strategic Policy and Intelligence (DEPSEC SP&I)

48. DEPSEC SP&I is responsible for approving offsite work involving the handling, storage or disposal of information that is classified TOP SECRET or carries a CODEWORD.

CODEWORD Compartment Controllers

49. Compartment controllers are responsible for providing advice to DEPSEC SP&I 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.

50. For compartments managed on behalf of external agencies, compartment controllers are to liaise with those agencies on matters of shared security risk.

Executive Security Advisers (ESA)

51. Executive Security Advisers (ESA) are responsible for assessing the security arrangements for, and managing any accreditation of, home-based work arrangements for Defence personnel and persons engaged under contract employed in single-service units.

Commanders, Managers and Contract Managers

52. Commanders, Managers and Contract Managers are responsible for the approval of offsite work:

a. where physical storage is required for OFFICIAL 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).

Managers of person/s engaged under a contract

53. Managers of persons engaged under contract 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 involving Defence information or assets.

Key Definitions

54. **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.*

55. **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.

56. **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.

57. **Home-based Employee.** An employee working at a home-based site.

58. **Home-based Work Agreement.** A formal agreement between an employee and Defence documenting the conditions of home-based work.

59. **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.

60. **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.*

61. **Privately Owned Device.** 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.*

62. **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.*

63. **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.

64. **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; and

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

65. 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	4
Publication date	3 August 2020
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Working Offsite
Related DSPF Control(s)	Assessing and Protecting 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
2	09 April 2020	AS SPS	Foundational review; PSPF update; security classification alignment; update of terms defined in Defence Instruction: Administrative Policy; and update to align with flexible working arrangements during COVID-19.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF
4	3 August 2020	AS SPS	Update of dispensation DEFGRAM 315/2020

Australian Government
Department of Defence

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 persons engaged under contract; and

c. maintain a safe and secure working environment for Defence personnel and persons engaged under contract.

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: *Persons engaged under contract 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	4
Publication date	14 March 2025
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	PSPF Standards

Version control

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

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	22 September 2020	FAS S&VS	Control Owner transferred to AS STA on 31 August 2020
4	14 March 2025	FAS DS	Control Owner transferred to AS SPS on 17 February 2025

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 AS SPS has set the following general thresholds for risks managed against this DSPF Enterprise-wide Control and the related DSPF Principle and Expected Outcomes.

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: *Persons engaged under contract 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 Protective Security Policy Framework (PSPF) sets out the minimum physical security controls required for protecting security-protected assets (refer to Key Definitions). These controls provide a level of assurance of which information originators and asset owners need in order to be confident the information and assets they share with others is protected at the standard required by government.

4. PSPF policy and guidance is at:

a. PSPF Annual Release

b. Defence Security Guidance tools and templates- ASIO Technical Note 1/15 (Physical Security of Zones 2 - 4)

c. Defence Security Guidance tools and templates - ASIO Technical Note 5/12 (Physical Security of Zone 5 - TS Areas)

d. Australian Government physical security guidelines (Facilities and systems)

e. Guidelines for ICT equipment

Information Originators and Asset Owners

5. Originators of information and asset owners are to determine the appropriate Business Impact Level (BIL) to be applied to the confidentiality, integrity and/or availability for the information or asset. As this process is to be in accordance with BILs, refer to PSPF Annual Release.

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 – *Assessing and Protecting 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 Physical Security Zone (Security Zone) for the protection of security protected assets based on the classification or BIL of the information or asset(s) (refer to *Identification of Security Zones* in this DSPF Control). 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, policy 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 should be substantiated through their formal security risk management plan. This may include the need to store and handle the information or 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 Managers (BMs). 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 the 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 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.

12. 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 and Sections are to seek advice from Defence Security Division (DS Division) or relevant Executive Security Advisor (ESA) before installing a commercial vault or strong room for the protection of security-protected assets.*

13. 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.

14. 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 measures are further defined using the Security Zone methodology described within the PSPF.

15. For further information on application of access control, refer to the DSPF Principles for:

a. *74 - Access Control*;

b. *10 - Classification and Protection of Official Information*; and

c. *40 - Personnel Security Clearance*.

Security Zones

16. Security Zones describe areas on a site that process, handle and store security-protected assets and information. They are designed to protect security-protected assets of a specific BIL.

17. The primary outcome of the Security Zone methodology (refer to PSPF Policy 16 *Entity Facilities*) 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

18. Base or site planning involves assessing and identifying areas requiring a Security Zone. Where required, assistance should be sought from their Security Officers, DS Division or relevant Executive Security Advisor (ESA).

19. Commanders and/or Managers of the business unit/area along with the asset custodians, in consultation with system owners and other relevant stakeholders (such as Senior Australian Defence Force Officers and Heads of Resident Units or their Security Officer), are responsible for assessing their Security

Zone requirements. This includes identifying any changes required to meet DSPF requirements on a base or within a facility that processes, handles and/or stores security-protected assets. Such areas should be categorised according to the Security Zone methodology described within PSPF guidelines (refer to PSPF Annual Release).

To assist units in understanding zoning requirements staff should access:

a. the Physical Security Zone Assessment Tool, an interactive PDF that provides guidance to help staff understand what Zone they should be working in to meet their business needs;

b. their Group or Service ESA; or

c. their local Directorate of Security Assurance (DoSA) regional office for specific subject matter expertise in work area guidance and advice.

20. Once Security Zones have been identified and categorised, facility owners **must** seek certification and accreditation of those Security Zones by the appropriate authorities, in accordance with DSPF Principle 73 – *Physical Security Certification and Accreditation*.

21. In an area of operations, it is recommended the relevant Task Force Commander appoint an individual to identify and categorise those areas that process, handle and store security-protected assets.

22. Areas within a site that are not used to process, handle or store security-protected assets are not required to be categorised.

23. 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 the PSPF Annual Release.

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.*

Facility Design and Development (including Greenfield Sites)

24. 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 Division or the relevant ESA. Greenfield sites are for new projects identified to process, handle and store security-protected assets and are to be categorised and accredited using the Security Zone methodology described above.

Prohibition of SECRET Business in Zone Two Areas

25. In accordance with the Government PSPF security standard, the DSPF prohibits all SECRET business in Zone Two areas. This includes discussions, storage and use of hard and soft copy SECRET material. Additionally, Defence Secret Network (DSN) Terminals cannot be used or stored in a Zone Two area.

Portable Electronic Devices – Usage in Zones

26. Portable Electronic Devices (PEDs) are devices that can capture, process, store, record or communicate information electronically.

27. The Chief Information Security Officer is the policy authority for the specific use of ICT (including PEDs) in Defence. DSPF Principle 21-Information and Technology Security (Physical) and Joint Capabilities Group's Management Guidance for Portable Electronic Devices in Defence Security Zones **must** be referred to for information on appropriate PED usage in Zones.

28. All Zone Three areas are PED-restricted areas under the DSPF. Zone Four and Five areas are PED-prohibited areas (ISM control 0225), with exceptions for certain medical and approved portal devices. Any devices in Zone Five SCIFs must be approved by the Australian Signals Directorate.

Control Requirements

29. PSPF Annual Release, 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.

30. The risk mitigation control requirements, which are outlined in PSPF policy: PSPF Annual Release 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., an SRA is to be conducted to determine additional prescriptions above the minimum for any Security Zone.

Security Clearance Requirements for Access to Security Zones

31. 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 an SRA.

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 **must** be escorted at all times within these Zones.*

Alternative Storage Arrangements for Security Protected Assets

32. 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 SRA; and

c. meet the business needs of the asset owner/custodian.

33. Where an asset is classified, it is to be stored in the same way as information of the same classification, (refer to PSPF Annual Release). 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 Division or the relevant ESA can be contacted for advice.

34. Where it is impractical altogether to store classified assets in a secure facility, these are to be protected from unauthorised access, surveillance and theft. DS Division or the relevant ESA can be contacted for advice, which 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.

35. 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.

36. 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 should be obtained from the Australian Signals Directorate.

Storage of High-Risk Official and Unclassified Assets

37. It is recommended that high-risk official 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 security containers and vaults for storing assets.

38. 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 Joint Operations Command (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.

39. Where it is impractical altogether to store high-risk Official assets in a secure facility, they should be protected from unauthorised access, surveillance and theft. DS Division or the relevant ESA can be contacted for advice.

Guarding and Patrol Requirements

40. 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

41. 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 SRA dictates otherwise.

42. 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.*

43. 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

44. 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.

45. 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.*

46. 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 SRA 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

47. 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.

48. 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

53. Australian Defence Force (ADF) platforms, due to varying designs, may not conform to the technical specifications described in the PSPF Annual Release 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

54. **Physical Transfer**. Security-protected assets are to be transported in accordance with DSPF Principle 71 – *Physical Transfer of Information and Assets*.

55. **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.

56. **Disposal**. Classified assets are to be disposed of in accordance with DSPF Principle 10 – *Classification and Protection of Official Information*. High risk official 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.

57. **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.*

58. **Special Access Programs**. Additional requirements for the handling of security-protected assets relating to the Defence Special Access Program are detailed in *Directive 19/2023 – The Defence Special Access Program Framewor*.

Roles and Responsibilities

Project Managers

59. Project Managers (for Defence Industry, this applies to Contract Managers), who are responsible for construction or refurbishment projects, are responsible for compliance with this DSPF Principle and the source material it references. For further information regarding project security, refer to DSPF Principle 11 – *Security for Projects*.

Facility Owners

60. Facility owners, including Base Managers (BM), 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 facilities 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 Group or Service.*

Asset Custodians

61. 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 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 Principle; and

d. ensuring that employees or persons engaged under contract 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

62. 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

63. Contract Managers are responsible for:

a. the acceptance of physical security risks arising from the storage of official information and security-protected assets at persons engaged under contract facilities; and

b. ensuring that Defence assets are protected in accordance with this DSPF part when those assets are in the possession of persons engaged under contract.

Key Definitions

64. **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.

65. **Asset owner**. The Group Head or Service Chief with responsibility and accountability for an asset for which responsibility has been assigned to them.

66. **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, PSPF Annual Release.

67. **Facility owner**. The person responsible for the operation of a facility.

68. **Greenfield**. In the physical security context, a Greenfield site is a property that has not undergone an Australian Government security treatment.

69. **Information originators**. The entity/ies responsible for creating and classifying Official Information.

70. **Official Information**. Any information received, developed or collected by, or on behalf of, the Australian Government, through its agencies and persons engaged under contract, 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.

71. **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).

72. **Security-protected asset**. A non-financial, reportable or accountable asset that requires greater than standard fire and theft protection due to either:

a. being allocated a BIL of 2 (Low to Medium) or higher;

b. an unacceptable business impact that would result from the unauthorised modification (i.e. loss of integrity) of the asset, irrespective of whether that modification can be detected or not;

c. an unacceptable business impact that would result from the asset being unavailable (i.e. loss of availability) for a given period of time; or

d. being categorised as a weapon or explosive ordnance.

73. **Security Zones**. A methodology for physical security mitigation based on an SRA. 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.

74. **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.

75. **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.*

Further Definitions

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

77. Definitions for common Defence administrative terms can be found in the Defence Instruction.

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	6
Publication date	14 March 2025
Type of control	Enterprise-wide
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Physical Security
Related DSPF Control(s)	Control 21.1 – Information and Technology Security (Physical) Control 22.1 – Mobility Device Security Control 73.1 – Physical Security Certification and Accreditation

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 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
3	22 September 2020	AS SPS	Control Owner transferred to AS STA on 31 August 2020
4	23 May 2024	FAS DS	Control updated to reflect changes to Zones Two and Three in the PSPF
5	17 December 2024	AS STA	Control updated to reflect JCG policy authority on Personal Electronic Devices
6	14 March 2025	FAS DS	Control Owner transferred to AS SPS on 17 February 2025

Australian Government
Department of Defence

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 core requirements for physical security 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 secure zones 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 zones. Information with an Information Management Marker (IMM) 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.

c. 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
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 2 (Low to Medium). Or limited holdings of information with an OFFICIAL: Sensitive Information Management Marker (IMM) (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 4 (Extreme). Or limited holdings of SECRET information	Not permitted	Not permitted (See note below for policy transition details)	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 2.c. above	Not normally permitted. (In exceptional circumstances SCEC Class B) see 2.c. above	SCEC Class B

Note: *Security classified material at the SECRET level currently stored in a Class A container within a Zone 2 must be relocated to a minimum Zone 3 by 1 August 2022.*

Safes and Vaults for Protection of High Risk Official 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 Official Assets (GUIDANCE ONLY)

High risk unclassified assets / categorised assets	Zone One	Zone Two	Zone Three	Zone Four
High risk official assets the loss of which would have a BIL of 1 (Low) or SUPPORT assets	Locked commercial container	Locked commercial container	Determined by a security risk assessment	Determined by a security risk assessment
High risk official assets the loss of which would have a BIL of 2 (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 official assets the loss of which would have a BIL of 3 (High) or IMPORTANT assets	Commercial safe or vault	Commercial safe or vault	Commercial safe or vault	Determined by a security risk assessment
High risk official assets the loss of which would have a BIL of 4 (Extreme) or MAJOR assets	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 official 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 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:

(1) the lock **must** be reset to the manufacturer's standard setting (usually 40-50-60 or as shown in the instruction book); and

(2) 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	4
Annex Publication date	31 July 2020
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
2	6 July 2020	AS SPS	Table 1 Security Containers for Official Information in Zone 2 aligned with PSPF.
3	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	18 September 2020	AS SPS	Transition policy for storage of SECRET information

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 and persons engaged under contract access; and Restricted public access	Zone Two
Accredited Partially Secure Area	Limited Defence personnel and persons engaged under contract access and escorted visitors only	Zone Three
Accredited Secure Area	Strictly controlled Defence personnel and persons engaged under contract access and escorted visitors only with an identified need to be there	Zone Four
Accredited TOP SECRET Areas	Strictly controlled Defence personnel and persons engaged under contract 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 and persons engaged under contract 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 official 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	2
Annex Publication date	31 July 2020
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
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy

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 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 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 Services (AS SPS)

Note: *Persons engaged under contract 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	5
Publication date	14 March 2025
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 73.1
Control Owner	Assistant Secretary Security Policy and Services (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 Assessing and Protecting 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	PSPF Standards

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 2048	FAS S&VS	Launch
2	17 July 2018	FAS S&VS	Corrected Control Owner designation
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	22 September 2020	FAS S&VS	Control Owner transferred to AS STA on 31 August 2020
5	14 March 2025	FAS DS	Control Owner transferred to AS SPS on 17 February 2025

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 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 Services (AS SPS)

Note: *Persons engaged under contract 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:

(1) classified information PROTECTED and above;

(2) Security Protected Assets with a Business Impact Level (BIL) of 3 (high) and above;

(3) ICT systems PROTECTED or above that are not protected by Australian Signals Directorate (ASD) endorsed encryption; and

(4) aggregated information with a BIL of 3 (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 separate 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: *DSD 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 OFFICIAL (including OFFICIAL: Sensitive 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 OFFICIAL: Sensitive 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 deployable facilities, and off-site areas such as home-based areas)	Joint, non-Service unit or DISP members' facilities.	DS(a)	DS(a)
Domestic - Security Zones One through to Four (including deployable facilities, and off-site areas such as home-based areas)	Single-Service Unit	ESA(b)	ESA(b)
Domestic – Commercial Shared Data centre facilities	In Australia on industry premises	DS(a)	DS(a)
Domestic - Security Zone Five Not including SCI	All Defence and Defence industry/DISP members	ASIO T4(c)	DS(a)
	Single-Service unit.	ASIO T4(c)	ESA(b)
Domestic – Compartments (k) within Zone Five	Joint, non-Service unit facility or DISP member's facility	DS(a)	DS(a)
	Single-Service unit	ESA(b)	ESA(b)
Domestic - SCI	All Defence and Defence industry/DISP members	ASIO T4(c)(i) (DSD to coordinate with ASIO T4(c) via submission of AE851(i))	ASD(d) 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(a)	DS(a)
	Single-Service unit. (not including overseas Areas of Operation)	ESA(b)	ESA(b)
	Overseas in Areas of Operation	CJOPS(e)	CJOPS(e)
ADF Platforms	Once in service or during regular maintenance or major	ESA(b)(h)	ESA(b)(h)

Facility	Location	Physical certification authority	Physical accreditation authority
	refit periods		
ADF Platform – SCI	Once in service or during regular maintenance or major refit periods	ASD(d) to coordinate	ASD(d) to coordinate
Overseas - All Security Zones Not including SCI	Zones 1 to 5 and compartments in a Zone 5 – internal to an Australian Diplomatic Mission. Not in Areas of Operation	DFAT(f)	DFAT(f)
	Zones 1 to 5 and compartments in a Zone 5 - external to an Australian Diplomatic Mission. Not in Areas of Operation	The DS(a) to coordinate(g) Note: DS consults DFAT and local certification authorities in accordance with a SIA(j)	The DS(a) to coordinate(g) Note: DS consults DFAT and local accreditation authorities in accordance with a SIA(j)
	Zones 1 to 5, and compartments in a Zone 5 In Areas of Operation	CJOPS(e)	CJOPS(e)
Overseas – SCI	SCI - All Defence and Defence industry/DISP members in and external to Australian Diplomatic Missions.	DS(a) to coordinate with ASD(d) and DFAT(a)	ASD(d) to coordinate
	SCI – in Areas of Operation	CJOPS(e) to coordinate with ASD(d)	ASD(d)

Notes:

(a) Defence Security.

(b) Executive Security Authority – For Navy, Army and Air Force.

(c) Certification activities undertaken by the Australian Security Intelligence. Organisation (ASIO) T4 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.

(d) Australian Signals Directorate SCIF Accreditation Team.

(e) Chief of Joint Operations (CJOPS) or authorised Delegate.

(f) Department of Foreign Affairs and Trade (DFAT).
(g) On occasions, the DS may delegate certification responsibility to the Chief Information Officer Group (CIOG), where CIOG is attending an overseas location to certify an ICT system.
(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.
(j) SIA - Security of Information Agreement or Arrangement
(k) Compartments are areas that require additional access control, including ICT server rooms and dedicated VTC rooms.

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, and projects involving the construction of ADF assets and platforms, it is recommended that consultation occur during planning and design 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:

(1) a Type 1A SAS commissioning certificate issued by a Security Construction and Equipment Committee (SCEC) Security Zone Consultant;

(2) an installation certificate for a commercial alarm system, which states compliance with Australian Standards AS/NZs2201 standard for Intruder Alarm Systems (not applicable for Zones Four or Five); or

(3) 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 and Managers that accreditation standards are maintained and identify any remediation where required. For DISP members, your Chief Security Officer (CSO) must complete an Annual Security Report (ASR) to meet DISP eligibility and suitability requirements.

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:

(1) changes to the BILs associated with the ICT system, information or assets handled or stored within;

(2) significant changes to the tenancy;

(3) changes in governance arrangements; or

(4) 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	Ten Years
Zone Three, Four and Five	Five 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 BILs of 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 assesment. 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 asset that requires greater than standard fire and theft protection due to either:

a. being allocated a BIL of 2 (Low to Medium) or higher;

b. an unacceptable business impact that would result from the unauthorised modification (ie. loss of integrity) of the asset, irrespective of whether that modification can be detected or not;

c. an unacceptable business impact that would result from the 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	9
Publication date	4 September 2025
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 Assessing and Protecting 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	02 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	06 August 2018	AS SPS	Giving CJOPS authority over EO storage and Armouries in areas of Ops
4	8 August 2019	AS SPS	PSPF alignment; Update to Reaccreditation intervals (Table 2)
5	22 May 2020	AS SPS	Update notes to explain acronyms in Table and amendments to para 15 reflect the requirement for DISP members to complete an annual security report
6	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
7	22 September 2020	AS SPS	Control Owner transferred to AS STA on 31 August 2020
8	14 March 2025	FAS DS	Control Owner transferred to AS SPS on 17 February 2025
9	4 September 2025	ESP	Updated broken hyperlinks

Australian Government
Defence

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

Document administration

Identification

DSPF Principle	Radioactive Sources
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 80
Version	4
Publication date	16 September 2025
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
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	16 September 2025	ESP	Updated Radiation manual link

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

Document administration

Identification

DSPF Principle	Fuel Security
Principle Owner	First Assistant Secretary Security and Vetting Service (FAS S&VS)
DSPF Number	Principle 84
Version	2
Publication date	31 July 2020
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
2	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy