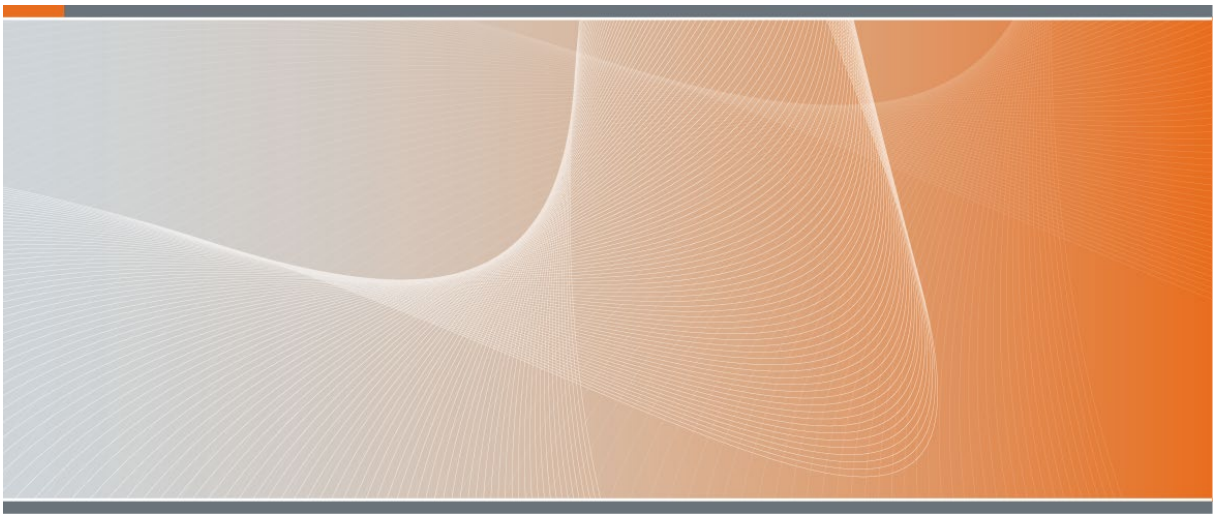
Australian Government
Defence

DEFENCE SECURITY PRINCIPLES FRAMEWORK



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

Department of Defence
CANBERRA ACT 2600

27 March 2025

Defence Security Principles Framework (DSPF)

Public Release Version

Note: *This document contains three DSPF Principles: 10 – Classification and Protection of Official Information, 11 – Security for Projects, and 16 – Defence Industry Security Program. Defence Industry Security Program (DISP) members may access the full DSPF through the Defence Online Services Domain (DOSD). Non-DISP members with a current ABN may request a version from Defence Industry Security Branch (DISB) Memberships; requests will need to be accompanied by a business case.*

Contents

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. The **Chief Security Officer**, as FAS DS, 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 65).

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 37).

30. **Control Owners** (refer paragraph 65) 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

35. 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.

36. Security risks are managed under the DSPF through:

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

Mandatory Provisions

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

38. 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.

39. 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

40. 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.

41. 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 63).

42. 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).

43. 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.

44. 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.

45. 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.

46. 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 69) and **Control Officers** (refer paragraph 72) 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

47. 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**.

48. The enterprise-wide security risk view is underpinned by assurance reporting from **Control Owners** (refer paragraph 65). **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.

49. 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.

50. 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

51. 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.

52. 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 LXP; and
- The appropriate document handling course.

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

Roles and Responsibilities

54. 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

55. 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

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

57. 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.

58. This includes key oversight responsibilities outlined in the *PSPF – Entity Protective Security Roles and Responsibilities*.

59. 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

60. 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.

61. 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**.

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

Defence Security Committee

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

64. 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 65) and enterprise-wide security risk reports; and

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

Control Owner

65. 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.

66. **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).

67. **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.

68. Where a **Control Owner** cannot be agreed, the ownership will be referred to the **DSC** (refer paragraph 63).

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

69. 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*.

70. **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**.

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

Control Officers

72. **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.

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

74. 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

75. 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

76. **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.

77. 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*.

78. 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.

79. 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	Assistant Secretary Security Policy 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	Classification and Protection of Official Information
Principle Owner	First Assistant Secretary Defence Security (FAS DS)
DSPF Number	Principle 10
Version	5
Publication date	31 March 2026
Releasable to	Defence, Defence Industry, and Public
Underlying DSPF Control(s)	Control 10.1
Control Owner	AS SPS

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)	21 - Information and Technology Security (Physical) 22 - Information and Technology Security (Personnel) 25 - Information and Technology Security (Gateways & Data Transfers) 40 - Personnel Security Clearance 44 - Overseas Travel 70 - Working Offsite 71 - Physical Transfer of Information and Assets
Implementation Notes, Resources and Tools	Business Impact Level Assessment Tool Security Classification and Categorisation Guide

Version control

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

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	31 May 2019	FAS S&VS	Foundational review; PSPF update; and security classification alignment.
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
5	31 March 2026	FAS DS	Updated 'releasable to'

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 D 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 F 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 Information and Communications Technology (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 Annex B 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 I 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 Defence Secret Network (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 C 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 E 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 G 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 to Table 1: Business Impact Levels for further information.

Australian Signals Directorate (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*

Annex J – *Creating and Managing Information Compartments*

Document administration

Identification

DSPF Control	Classification and Protection of Official Information
Control Owner	AS SPS
DSPF Number	10.1
Version	9
Publication date	31 March 2026
Type of control	Enterprise-wide
Releasable to	Defence, Defence Industry, and Public
General Principle and Expected Outcomes	Classification and Protection of Official Information
Related DSPF Control(s)	15 - Foreign Release of Official Information 21 - Information and Technology Security (Physical) 22 - Information and Technology Security (Personnel) 25 - Information and Technology Security (Gateways & Data Transfers) 40 - Personnel Security Clearance 44 - Overseas Travel 70 - Working Offsite 71 - Physical Transfer of Information and Assets 72 - Physical Security 77 - Security Incident Management and Investigation
Implementation Notes, Resources and Tools	*Archives Act 1983* Certificate of Assurance for Access to Australian Government Access Only (AGAO) information by United States, United Kingdom, Canadian or New Zealand nationals Defence Instruction Defence Records Management Policy Information Security Manual Security business impact levels

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.
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.
8	18 July 2025	AS SPS	Correction of Annex references
9	31 March 2026	AS SPS	Updated 'releasable to', moved hyperlinks to 'Implementation Notes, Resources and Tools'

Australian Government
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 DSPF Control 11.1 – *Security for Projects*, alongside other risk under Accountable Authority Instruction 1 - Managing Risk and Accountability. The DSPF 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 Strategy and Project Management Branch (AS SPM) through Branch Head (or equivalent)
High	Defence Security Committee (DSC) – through AS SPM
Extreme	DSC – through AS SPM

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 AS SPM.

Document administration

Identification

DSPF Principle	Security for Projects
Principle Owner	First Assistant Secretary Defence Security Division (FAS DS)
DSPF Number	Principle 11
Version	4
Publication date	31 March 2026
Releasable to	Defence, Defence Industry, and Public
Underlying DSPF Control(s)	Control 11.1
Control Owner	AS SPM

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 Program; 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; 20 – Information and Technology Security (Log Management); 21 – Information and Technology Security (Physical); 22 – Information and Technology Security (Personnel); 23 – Cyber Security Assessment and Authorisation; 40 – Personnel Security Clearance; 41 – Temporary Access to Classified Information and Assets; and 71 – Physical Transfer of Information and Assets.
Implementation Notes, Resources and Tools	Accountable Authority Instruction 1 - Managing Risk and Accountability ASIO Tech Notes via the Security Toolkit. Defence Integrated Investment Program 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). Security Equipment Guides (SEGs) via the Security Toolkit. The Defence Industry Security Program.Security Equipment Guides (SEGs) via the Security Toolkit.

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.
4	31 March 2026	FAS DS	Updated 'releasable to', and Control Owner title from AS FD to AS SPM

Australian Government
Defence

Defence Security Principles Framework (DSPF)

Security for Projects

Control Owner

1. The Assistant Secretary Strategy and Project Management (AS SPM) 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) is the Policy Owner for security.

2. The AS SPM 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 AS SPM 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	AS SPM through Branch Head (or equivalent)
High	Defence Security Committee (DSC) – through AS SPM
Extreme	DSC – through AS SPM

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 AS SPM.

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 (Communication Security (COMSEC) and Defence Information Environment architects);

d. Information and Communications Technology (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 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 Defence Industry Security Program (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 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 Management intranet section; 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 intranet section.

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. 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 Division 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 Division 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 Division at project.security@defence.gov.au.*

Roles and Responsibilities

First Assistant Secretary Defence Security Division

35. FAS DS 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 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 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 Defence Cyber and Information Assurance Branch 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 Chief Information Officer Group (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 Framework 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

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

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

Document administration

Identification

DSPF Control	Security for Projects
Control Owner	AS SPM
DSPF Number	Control 11.1
Version	4
Publication date	31 March 2026
Type of control	Enterprise wide
Releasable to	Defence, Defence Industry, and Public
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; 20 – Information and Technology Security (Log Management); 21 – Information Systems (Physical) Security; 22 – Information Systems (Personnel) Security; 23 – Cyber Security Assessment and Authorisation; 40 – Personnel Security Clearance; 41 – Temporary Access to Classified Information and Assets; 71 – Physical Transfer of Information and Assets; 73 – Physical Security Certification and Accreditation; and 82 – Procurement.

DSPF Control	Security for Projects
Implementation Notes, Resources and Tools	Services | Capability Acquisition and Sustainment Group Accountable Authority Instructions Project Controls - Schedule and Cost One Defence Capability System Defence Security Principles Framework Security services | Security and Estate Group Project Security Instructions (PSI) Business Impact Levels Special Access Program Framework Defence Instruction – Administrative Policy

Version control

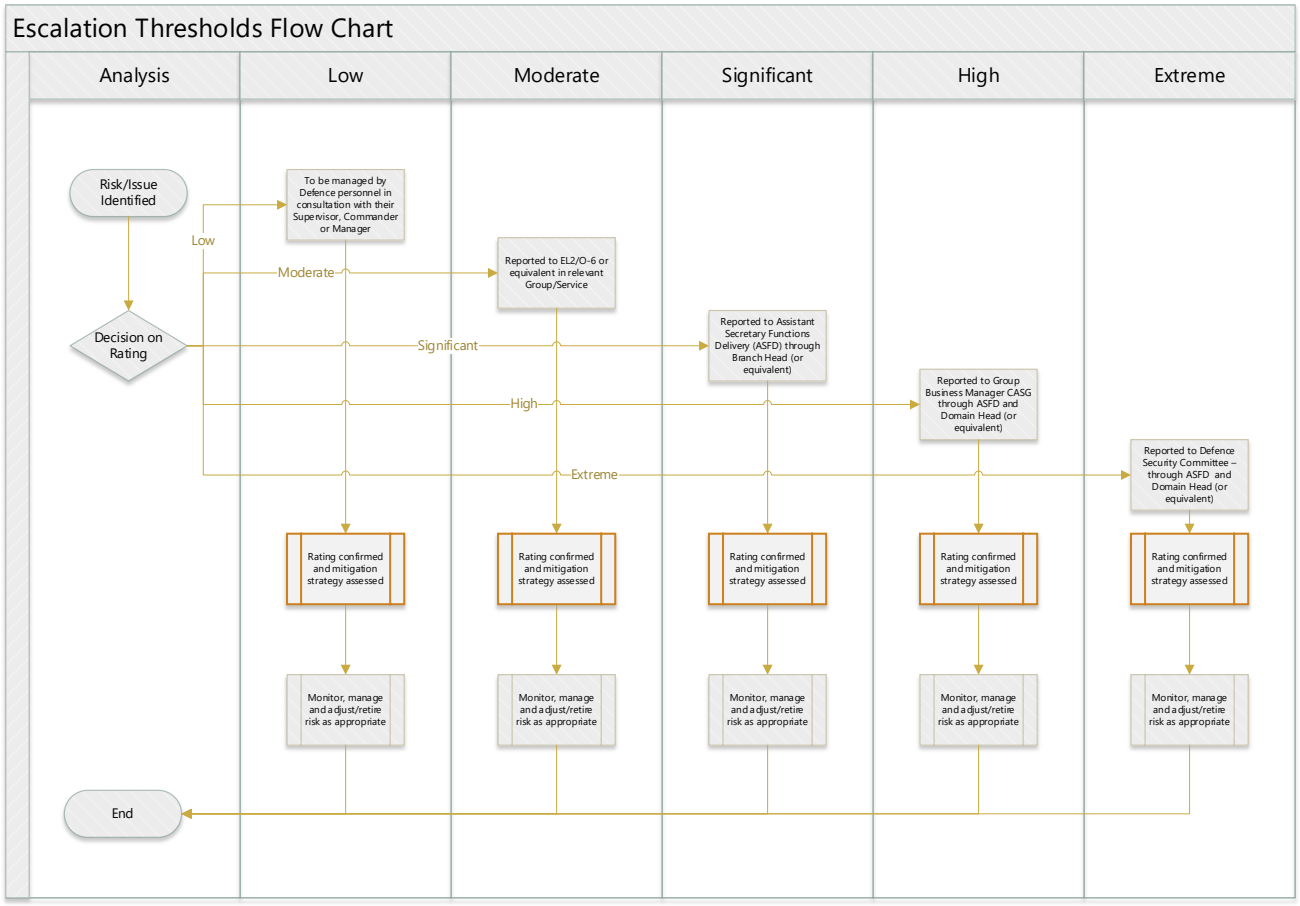
Note: A new row is added for each version to show the version history of this document.

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.
4	31 March 2026	AS SPM	Updated 'releasable to', updated related Principle/Control titles, updated Control Owner title from AS FD to AS SPM, and moved hyperlinks to 'Implementation Notes, Resources and Tools'

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	2
Annex Publication date	31 March 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	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
2	31 March 2026	AS SPM	Updated ‘releasable to’

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

Annex C – Special Access Programs

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 requirements 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’

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	3
Annex Publication Date	16 March 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	27 September 2024	AS DIS	Launch
2	29 January 2026	AS DIS	Updated references and links to SAP Framework
3	16 March 2026	AS DIS	Updated ‘Releasable to’