Defence Security Principles Framework (DSPF)

Defence Industry Security Program

Public version: *Classified content has been removed from this DSPF Principle. To view the full DSPF, visit the Defence Online Services Domain (DOSD) or contact the Defence Industry Security Program (DISP) Directorate.*

Contents

Defence Security Principles Framework (DSPF)

Defence Industry Security Program

General Principle

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

Rationale

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

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

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

Expected Outcomes

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

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

Escalation Thresholds

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

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

Document Administration

Identification

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

Related Information

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

Version Control

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

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	9 April 2019	FAS S&VS	DISP Reform Launch
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
4	17 February 2022	FAS DS	Enhancements to Defence Industry Security Program to improve the uplift of industry security and engagement
5	23 September 2022	FAS DS	Updates to Escalation Thresholds and Government Compliance
6	24 November 2023	FAS DS	Transfer of Control Ownership from AS SPS to AS DIS
7	27 September 2024	FAS DS	Update to “Related information” and to the Escalation Threshold table.
8	29 January 2026	FAS DS	Updated title, ‘releasable to’ and hyperlinks

Defence Security Principles Framework (DSPF)

Defence Industry Security Program

Control Owner

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

Escalation Thresholds

2. AS DIS has set the following general thresholds for risks managed against this *DSPF Enterprise-wide Control* and the related *DSPF Principle and Expected Outcomes*.

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

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

About the Defence Industry Security Program

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

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

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

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

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

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

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

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

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

c. provide security services for Defence bases or facilities;

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

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

6. The exception to this requirement is where:

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

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

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

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

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

Membership levels

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

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

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

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

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

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

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

DISP membership

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Suitability considerations

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

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

a. personnel security checks of nominated security staff;

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

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

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

d. Security Officer training for nominated security staff;

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

f. Physical accreditation (depending on membership level);

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

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

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

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

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

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

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

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

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

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

Refusing DISP membership

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

DISP membership fees

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

Ongoing DISP membership requirements

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

Ongoing security obligations

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

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

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

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

c. complete an Annual Security Report (ASR).

Ongoing reporting obligations

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

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

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

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

DISP uplift, remediation and assurance program

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

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

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

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

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

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

Non-compliance

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

Escalation pathway

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

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

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

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

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

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

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

Limiting DISP membership

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

Downgrading DISP membership

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

Suspending DISP membership

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

Termination of DISP membership

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

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

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

b. sponsor new and current Personnel Security Clearances;

c. receive security classified information, materials or assets;

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

e. engage in Defence projects requiring DISP membership;

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

g. use any DISP membership branding.

Procedure for membership modification by DISP member

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

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

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

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

Voluntary suspension or withdrawal from DISP

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

Procedural Fairness

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

Appeals and reviews

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

Roles and responsibilities

Defence

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

a. act in good faith;

b. act in the national interest;

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

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

e. uphold responsibilities under Commonwealth and Defence policy.

Defence Industry Security Branch

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

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

b. processing DISP membership applications;

c. providing ongoing security management advice; and

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

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

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

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

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

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

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

Contract Managers

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

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

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

Industry Entities

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

a. acting in good faith;

b. ensuring information provided is not deceptive or misleading;

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

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

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

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

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

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

   iii. maintaining communication with DISB.

Chief Security Officer

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

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

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

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

66. The CSO is accountable for ensuring:

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

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

c. DISP reporting obligations are fulfilled;

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

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

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

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

Security Officer

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Defence Industry Security Program Privacy Notice

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

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

Appropriate use of DISP branding

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

Additional Resources

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

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

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

Key Definitions

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Annexes

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

Annex B – Defence Industry Security Program – Contacts and

Resources

Document Administration

Identification

Control	Defence Industry Security Program
Control Owner	Assistant Secretary Defence Industry Security
Control Version	10
Publication date	29 January 2026
Releasable to	Defence, Defence Industry, and Public
Underlying DSPF Principles	Personnel Security Clearance Temporary Access Classification and Protection of Official Information Systems Security Cyber Security Assessment and Authorisation Foreign Release of Official Information Physical Transfer of Information, and Assets Security Incidents and Investigations Procurement

Version Control

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

Version	Date	Author	Description of changes
1	2 July 2018	AS SPS	Launch
2	9 April 2019	AS SPS	DISP Reform Launch
3	10 April 2019	AS SPS	Update
4	31 July 2020	AS SPS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy
5	17 February 2022	AS SPS	Rewritten policy to improve the uplift of industry security and engagement
6	1 August 2022	AS SPS	Update to Escalation Threshold table, DRICS reference, workplace standard, and Entry Level and Level 3 membership requirements
7	30 March 2023	AS SPS	Update Paragraph 21 clarifying email address requirements for DISP members/applicants.
8	24 November 2023	FAS DS	Transfer of Control Ownership from AS SPS to AS DIS
9	27 September 2024	AS DIS	Refresh text to reference the Defence Industry Security Branch and the DISP Member Portal; update mandatory membership provisions; clarify CSO and SO PSC requirements; upgrade cyber security requirements; include Special Access Programs Annex.
10	29 January 2026	AS DIS	Updated ‘releasable to’

Defence Security Principles Framework (DSPF)

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

Conditions applicable to all Industry Entities

1. All Industry Entities must:

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

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

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

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

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

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

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

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

Membership Level Requirements

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

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

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

		clearances up to and including the Baseline level.		

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

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

Relevant DSPF Controls

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

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document Administration

Identification

Annex	Defence Industry Security Program – DISP Membership Requirements
Annex Version	7
Annex Publication Date	29 January 2026
Releasable to	Defence, Defence Industry and Public
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Industry Security Program
DSPF Principle	Control 16.1

Version Control

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

Version	Date	Author	Description of changes
1	9 April 2019	AS SPS	DISP Reform Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	17 February 2022	AS SPS	Replacement of previous Annex A - Privacy Notice
4	4 March 2022	AS SPS	Update to clarify clearance sponsorship eligibility for each DISP level
5	1 August 2022	AS SPS	Update to workplace standard, and Entry Level and Level 3 membership requirements
6	27 September 2024	AS DIS	Update references and change minimum cyber security standards.
7	29 January 2026	AS DIS	Updated ‘releasable to’ and relevant DSPF Control references

Defence Security Principles Framework (DSPF)

Annex B to Defence Industry Security Program – Contacts and Resources

DISP Contacts

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

Resources

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

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document Administration

Identification

Annex	Contacts and Resources
Annex Version	5
Annex Publication Date	29 January 2026
Releasable to	Defence, Defence Industry and Public
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Industry Security Program
DSPF Principle	16

Version Control

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

Version	Date	Author	Description of changes
1	9 April 2019	AS SPS	DISP Reform Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF
3	17 February 2022	AS SPS	Replacement of previous Annex B – Suitability Matrix
4	27 September 2024	AS DIS	Update of links and contacts.
5	29 January 2026	AS DIS	Updated ‘releasable to’

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’