Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Defence Industry Security Program

General Principle

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

Rationale

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

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

4. DISP sets minimum security standards required for industry to partner on projects at the 'OFFICIAL', 'OFFICIAL: Sensitive', 'PROTECTED', 'SECRET' and 'TOP SECRET' levels.

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

Expected Outcomes

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

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

8. DISP:

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

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

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

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

Escalation Thresholds

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

Note: *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 Program
Principle Owner	First Assistant Secretary Security and Vetting Service
DSPF Number	Principle 16
Version	3
Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Underlying DSPF Control(s)	Control 16.1
Control Owner	Assistant Secretary Security Policy and Services

Related information

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

Version control

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

Version	Date	Author	Description of changes
1	2 July 2018	FAS S&VS	Launch
2	9 April 2019	FAS S&VS	DISP Reform Launch
3	31 July 2020	FAS S&VS	Protective Marking update to align with PSPF; update of language to reflect Defence Admin Policy

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Defence Industry Security Program

Control Owner

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

Escalation Thresholds

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

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

The Program

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

3. The exception to this is where an Entity:

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

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

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

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

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

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

Membership

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

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

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

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

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

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

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

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

Eligibility

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

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

b. be financially solvent;

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

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

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

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

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

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

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

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

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

Suitability

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

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

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

18. The DISP Suitability Matrix at Annex B of this Control specifies the minimum membership requirements for each level and element of the DISP. Applicants self-

nominate the membership level that best meets their entity's requirements.

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

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

Ongoing Suitability

21. DISP members **must**:

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

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

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

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

(1) eligibility and suitability changes;

(2) FOCI changes;

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

(4) contact with foreign officials; and

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

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

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

Security Incident & Foreign Contact Reporting

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

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

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

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

Upgrading or Downgrading Membership

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

Contract Managers

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

a. the Defence representative contact details;

b. the Entity Defence is engaging with;

c. details of the contract/panel/partnership;

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

Assurance

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

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

b. Annual Security Report (ASR);

c. Intelligence led assurance program;

d. Five year forward audit work program, and

e. Shipbuilding assurance program.

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

a. undertake assurance and compliance activities;

b. review DISP member’s ASR annually;

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

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

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

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

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

International Recognition

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

32. These allow for:

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

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

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

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

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

Australian Community

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

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

Prioritisation Framework

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

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

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

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

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

Roles and Responsibilities

Defence

39. Defence is responsible for:

a. acting in good faith;

b. providing information and support for joining the DISP;

c. processing membership applications in a timely manner;

d. providing ongoing security management advice;

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

f. providing vetting services through AGSVA; and

g. upholding all responsibilities as per the policy framework.

Industry Entities

40. Industry Entities are responsible for:

a. acting in good faith;

b. ensuring information provided is not deceptive or misleading;

c. applying the 'need to know principle';

d. ensuring no unauthorised access (including by third parties) to Official Information or materials;

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

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

Chief Security Officer

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

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

43. The CSO is accountable for ensuring:

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

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

c. DISP reporting obligations are fulfilled;

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

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

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

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

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

Security Officer

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

46. The SO is responsible for:

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

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

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

d. the management of personnel security clearance requests;

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

f. facilitating annual security awareness training of personnel;

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

h. yearly assurance activities to support the CSO.

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

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

Ceasing Industry Security Program Membership

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

Voluntary withdrawal or ceasing

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

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

Terminating, suspending or downgrading membership

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

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

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

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

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

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

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

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

Obligations and Consequences

58. When DISP membership ceases:

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

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

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

d. facility and ICT system accreditation will lapse; and

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

Dispute Resolution, Procedural Fairness, Appeals and Reviews

Dispute resolution

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

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

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

Procedural Fairness

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

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

64. At any time, if a significant security concern is identified, notwithstanding procedural fairness provisions, FAS S&VS retains the right to temporarily suspend or remove an Entity's access to security services, including suspension or termination of Physical or ICT certification, accreditation and/or withdrawing sponsorship of personnel security clearances and the ability to sponsor clearances.

Appeals and Reviews

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

Key Definitions

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

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

Annexes

Annex A – Defence Industry Security Program – Privacy Notice

Annex B – Defence Industry Security Program – Suitability Matrix

Document administration

Identification

DSPF Control	Defence Industry Security Program
Control Owner	Assistant Secretary Security Policy and Services
DSPF Number	Control 16.1
Version	4
Publication date	31 July 2020
Type of control	Enterprise
Releasable to	Defence and Defence Industry
General Principle and Expected Outcomes	Defence Industry Security Program
Related DSPF Control(s)	Personnel Security Clearance Temporary Access Assessing and Protecting Official Information Information Systems Security 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

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex A to Defence Industry Security Program – Privacy Notice

Defence Industry Security Industry Program Privacy Notice

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

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

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

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

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

a. Other Government agencies; or

b. International Partners under an SIA.

The purpose for collecting your information

4. Personal information is collected to assess your entities eligibility to hold and maintain DISP membership. It is important to note that failure to provide accurate information required for this assessment may result in a failure to obtain DISP membership and will impede on your ability to apply for DISP membership in the future. Your company information may also be used in the identification, management and investigation of security threats and incidents and to undertake investigations into suspected breaches of law or of Australian Government policy.

Accessing and updating your information

5. For information about how Defence holds your personal information, how you can apply for access to, or seek a correction of personal information Defence holds about you, or to make a complaint about how Defence has managed your personal information, you should refer to the Defence Privacy Policy.

6. Questions regarding the Defence Privacy Policy, or privacy within Defence, should be emailed to the Defence Privacy Office defence.privacy@defence.gov.au or sent via regular mail to:

Defence Privacy Office
BP35-1-065
PO Box 7927
CANBERRA BC ACT 2610

Additional Resources

7. The *Privacy Act 1988*

Further information can be found at Defence Privacy Policy.

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments

Document administration

Identification

DSPF Annex	Defence Industry Security Program – Privacy Notice
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Industry Security Program
DSPF Number	Control 16.1

Version control

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

Version	Date	Author	Description of changes
1	9 April 2019	AS SPS	DISP Reform Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF

Australian Government
Department of Defence

Defence Security Principles Framework (DSPF)

Annex B to Defence Industry Security Program – Suitability Matrix

	Governance*	Personnel Security	Physical Security	Information and Cyber Security
Entry Level	• Maintain an appropriate system of risk oversight and management (i.e. risk register including security considerations). • Provide business details • Provide points of contact • Must have a nominated Chief Security Officer (CSO) (must be able to meet AGSVA eligibility requirements for Baseline clearance) • Must have a nominated Security Officer (SO) (must be able to meet AGSVA eligibility requirements for Baseline clearance) • SO may request access to the DISP Security Portal, to access security documents, templates, forms and tools which include: – assurance reporting forms, security policy and plans templates, risk assessment forms etc., • Security Officer Training Course is optional for nominated SO and CSO however the SO is to complete the Introduction to DISP course • Annual Security Awareness Course must be completed by all personnel • Security Officer must understand and effectively manage personnel/facilities and information and cyber security up to an 'OFFICIAL: Sensitive' level • Maintain and implement Security Policies and Plans • Insider threat program • Business security risk assessment • Reporting and management of security incidents and foreign contacts • Report changes in Foreign Ownership Control & Influence • Conduct travel briefings • Complete annual assurance activities • Annual Security Report	• SO has no ability to sponsor security clearances • Provide a description of employment screening practices • AS 4811—2006 Employment screening is the minimum standard for all new recruitments	• Provide a description of physical security and access controls at each facility and their location	• Must meet one of the following standards across all of the Entity's ICT corporate networks used to correspond with Defence: – The following four requirements of the ASD Essential 8: ○ application whitelisting; ○ patch applications; ○ restrict administrative privileges; and ○ patch operating systems – 'OFFICIAL: Sensitive' network in accordance with the ISM/DSPF – ISO/IEC 27001/2:2013 Information security management – NIST SP 800-171 Rev.1 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (US ITAR requirement) – Cyber security for defence suppliers (Def Stan 05-138) • Provide a description of information and cyber security practices and accreditations.

	Governance*	Personnel Security	Physical Security	Information and Cyber Security
Level 1	**All governance requirements from the Entry Level, plus:** • Complete annual assurance activities Security Officer required to maintain a NV1 clearance • Security Officer understands and effectively manages personnel/facilities and Information and cyber security up to and including 'PROTECTED' level • Security Officer Training Course is required for the SO, but optional for the CSO. • SO may request access to the Security Officer Dashboard for the ability to sponsor security clearances • Maintain a list of Designated Security Assessed Positions (DSAP)	**All personnel requirements from the Entry Level, plus:** • Security Officer has the ability to sponsor Baseline security clearances • Ensure Baseline cleared personnel adhere to ongoing security clearance requirements	**All physical requirements from the Entry Level, plus:** • Ensure facilities are certified and accredited in accordance with the DSPF to receive, handle, store and destroy 'PROTECTED' information and material	**All information & cyber requirements from the Entry Level, plus:** • Ensure a 'PROTECTED' network or standalone device is employed in accordance with the ISM/DSPF
Level 2	**All governance requirements from Level 1, plus:** • Security Officer must understand and effectively manage personnel/facilities and Information and cyber security up to and including 'SECRET' level	**All personnel requirements from the Entry Level, plus:** • Security Officer has the ability to sponsor security clearances up to NV1 • Ensure Baseline and NV1 cleared personnel adhere to ongoing security clearance requirements • Ensure compartment holders adhere to compartment requirements	**All physical requirements from the Entry Level, plus:** • Ensure facilities certified and accredited in accordance with the DSPF to receive, handle, store and destroy 'SECRET' information and material	**All information & cyber requirements from the Entry Level, plus:** • Ensure a 'SECRET' network or standalone device is employed in accordance with the ISM/DSPF
Level 3**	**All governance requirements from Level 2, plus:** • If applicable, Security Officer trained in compartment briefings obligations COMSO course • Security Officer must understand and effectively manage personnel/facilities, and Information and cyber security up to and including TOP SECRET level***	**All personnel requirements from the Entry Level, plus:** • Security Officer has the ability to sponsor security clearances up to NV2 • Ensure Baseline, NV1 and NV2/PV cleared personnel adhere to ongoing security clearance requirements • Ensure compartment holders adhere to compartment requirements	**All physical requirements from the Entry Level, plus:** • Ensure facilities certified and accredited in accordance with the DSPF to receive, handle, store and destroy TOP SECRET information and material	**All information & cyber requirements from the Entry Level, plus:** • Ensure a TOP SECRET network or standalone device is employed in accordance with the ISM/DSPF

* Governance security must always match or exceed the highest level of membership sought for any other category.

** SES Band 3 sponsorship is required to obtain a Positive Vetting clearance / certification and accreditation of Secure Compartment Information Facility (SCIF) and 'TOP SECRET' network.

*** Note: the management of compartment briefs will be managed by a Defence Communications Intelligence Security Officer (COMSO).

Appendixes and Attachments

This DSPF Annex has no Appendixes or Attachments.

Document administration

Identification

DSPF Annex	Defence Industry Security Program – Suitability Matrix
Annex Version	2
Annex Publication date	31 July 2020
Releasable to	Defence and Defence Industry
Compliance Requirements	Compliance requirements for this supplementary document are the same as for its parent document (DSPF Control).
DSPF Control	Defence Industry Security Program
DSPF Number	Control 16.1

Version control

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

Version	Date	Author	Description of changes
1	9 April 2019	AS SPS	DISP Reform Launch
2	31 July 2020	AS SPS	Protective Marking update to align with PSPF