Defence Security Principles Framework (DSPF)

Defence Industry Security Program (DISP)

Control Owner

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

Escalation Thresholds

<table>
<thead>
<tr>
<th>Risk Rating</th>
<th>Responsibility</th>
</tr>
</thead>
<tbody>
<tr>
<td>Low</td>
<td>Assistant Director Industry &amp; International Security Policy</td>
</tr>
<tr>
<td>Moderate</td>
<td>Director Industry &amp; International Security Policy</td>
</tr>
<tr>
<td>Significant</td>
<td>Assistant Secretary Security Policy and Services</td>
</tr>
<tr>
<td>High</td>
<td>First Assistant Secretary Security and Vetting Services</td>
</tr>
<tr>
<td>Extreme</td>
<td>Defence Security Committee (DSC) – through AS SPS</td>
</tr>
</tbody>
</table>

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

The Program

1. The Department of Defence (Defence) requires any Industry Entities to hold an appropriate level of DISP membership when working on sensitive or classified information or assets; storing or transporting Defence weapons or explosive ordnance; or providing security services for Defence bases and facilities; or as a result of a Defence business requirement.

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

3. 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’s security requirements. These services include personnel security vetting, certification and accreditation of facilities and/or ICT systems.

4. DISP membership supports industry partnerships and supply chain security.
5. Industry Entities can self-nominate to join DISP independently of having a contract with Defence.

Membership

6. To attain and maintain DISP membership, Industry Entities must meet eligibility and suitability requirements.

7. 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.

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

Eligibility

9. To be eligible for DISP membership an Industry 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 fulfill the role of a Chief Security Officer (CSO);i;
   d. have a designated officer who can fulfill the role of Security Officer (SO);ii; and
   e. have a contact email address to facilitate correspondence;
   f. not have any relationships with a listed terrorist organisation;iii
   g. complete the foreign, ownership, control and influence assessment;
   h. not have any relationship with regimes subject to Australian sanctions laws including the United Nations Security Council (UNSC) sanctions regimes and Australian autonomous sanctions regimes;iv
   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;v

10. Defence, through the First Assistant Secretary Security and Vetting Service (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 eligibility and suitability criteria are not met.

Suitability

11. An Industry Entity that meets the eligibility requirements can apply for DISP membership by submitting a DISP application and Foreign Ownership, Control and Influence (FOCI) form.

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

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

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

15. To be granted DISP membership an applicant must at least meet the minimum requirements for each element of the DISP at entry level.
16. 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 business needs or contract requirements. While personnel, physical and ICT/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

17. DISP members must:
   a. safeguard Defence and industry’s people, information and assets;
   b. comply with relevant DSPF controls, including its referenced authoritative documents;
   c. appoint and retain a CSO, and trained SO;
   d. report any changes that may affect their Defence Industry Security Program membership in accordance with the relevant requirements of the DSPF, including but not limited to:
      i. eligibility and suitability changes;
      ii. FOCI changes;
      iii. security and fraud incidents;
      iv. contact with foreign officials;
      v. changes in circumstances for their security cleared personnel (e.g. contact details, relationship status, financial changes etc.);
   e. meet ongoing security reporting requirements within the designated timeframe for membership level; and
   f. meet Defence initiated compliance and assurance requirements, including undertaking the annual Protective Security Self-Assessment (PSSA).

Security Incident & Foreign Contact Reporting

18. 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 DSPF or the Information Security Manual.
19. This includes occurrences that affect a DISP member.
20. A security incident must be reported by the DISP member in accordance with Defence Policy.
21. DISP members must keep a register of all security incidents, and make it available to Defence upon request.
22. DISP Members must report suspicious, ongoing, unusual and/or persistent contact with a foreign national(s), in accordance with Defence Policy.
23. DISP members must report on any overseas travel undertaken by individuals who hold a security clearance.

Upgrading or Downgrading Membership

24. 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.
Assurance

25. Contract Managers must notify DS&VS where DISP membership is a contract requirement. Contract managers must provide DS&VS with the following information:
   a. Project title
   b. Project/Contract Manager name and contact details
   c. DISP Membership Level required in contract: For example Governance level 'x', Personnel Security level 'x', Physical Security level 'x', ICT/Cyber Security level 'x'
   d. Contract duration
   e. Any additional security controls as a condition of contract

26. Participation in the DISP provides greater assurance to Defence when partnering with industry as members must meet additional controls not otherwise required in the DSPF.

27. Greater DISP participation by Defence's industrial supply chain will further improve Defence's assurance.

28. To ensure compliance with the DISP minimum security requirements, Defence will undertake the following assurance activities:
   a. undertake assurance and compliance activities;
   b. review DISP member’s PSSA annually;
   c. conduct random and targeted security spot 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;
   d. assess Industry security incident, fraud and contact reports, in accordance with DSPF; and
   e. conduct security investigations as appropriate, in accordance with DSPF.

29. The outcome of the assurance activities will also inform the CASG Company Performance ScoreCard rating.

International Recognition

30. 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.

31. 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.
   b. Foreign companies to participate in contracts generating or providing access to classified information in Australia even though they may not be DISP members.

32. To confirm the existence of an international Agreement or Arrangement, enquires should be directed to dsvsdsp.international@defence.gov.au.

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

Export Control

35. The export of strategic goods and technologies is managed by the export control office which is separate to the DISP. The Export Control Office can be contacted via ExportControls@defence.gov.au.

Roles and Responsibilities

Defence

36. 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;
   f. providing vetting services through AGSVA; and
   g. upholding all responsibilities as per the policy framework.

Industry Entities

37. Industry Entities are responsible for:
   a. acting in good faith;
   b. ensuring information provided is not deceptive or misleading;
   c. applying the “need to know principle”;
   d. ensuring no unauthorised access (including by third parties) to official/classified information or materials;
   e. providing all relevant information required to assess their eligibility and suitability for DISP membership; and
   f. where applicable, meeting all security requirements specified by Defence, and any Australian government entities or foreign government entities in contract and/or a Security of Information Agreement or Arrangement (SIA).

Industry Chief Security Officer

38. 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 level of DISP membership.

39. CSO is responsible for oversight of, and responsibility for, security arrangements and championing a security culture in the Industry Entity. They have the flexibility to delegate the day-to-day management of protective security to security officer/s, where required. CSO responsibilities include, but are not limited to, the below:
   a. implementing the requirements for the protection of classified information or materials up to the highest level of their DISP membership;
b. appointing a Security Officer who is responsible for the development and implementation of the security policies and plans and acts on behalf of the CSO. The CSO can also act as the SO; and

c. ensuring the implementation of any recommendations from annual assurance reporting.

Industry Security Officer

40. 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 level of DISP membership.

41. The SO is responsible for:
   a. the development and application of security policies and plans within the establishment;
   b. the management of personnel security clearance requests;
   c. reporting change of circumstances and vulnerabilities of clearance holders and any change in status of the legal entity;
   d. updating the register of personnel security clearances and access within the contracts. Register includes date of issue and expiry;
   e. providing DS&VS, at their request, information on all the personnel with security clearances;
   f. facilitating annual security awareness and training of personnel;
   g. reporting security incidents and fraud incidents in accordance with Defence policy; and
   h. yearly assurance reporting.

42. Industry Security Officers may not sponsor personnel security clearances requiring an eligibility waiver.

43. Where the exceptional circumstances criteria are met within the Australian Government’s Protective Security Policy Framework, Industry Security Officers are to consult with the control owner regarding clearance sponsorship for individuals requiring an eligibility waiver(s).

Ceasing Industry Security Program Membership

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

Voluntary withdrawal or ceasing

45. Industry Entities can voluntarily withdraw from the application process at any stage, or cease their membership by notifying Defence.

46. 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

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

48. 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, however, have other consequences, for example:
a. consequences that may arise because of a failure to comply with a contractual requirement, or
b. criminal or financial penalties or sanctions under Australian law.

49. A suspension is a time-limited operating constraint suspending that Industry Entity’s ability to operate as a DISP member. It may also prevent the Industry 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.

50. Downgrading or suspension can be imposed upon the whole business, an accredited facility or an ICT system. Personnel security clearances associated with the Industry 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 Industry 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.

51. Assistant Secretary Security Policy and Services (ASSPS) is to consult with affected parties prior to a decision to downgrade, suspend or terminate an Industry Entity’s DISP membership.

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

Obligations and Consequences

53. When DISP membership ceases:
   a. where applicable, any sensitive 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 of ceased memberships.

Dispute Resolution, Procedural Fairness, Appeals and Reviews

Dispute resolution

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

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

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

Procedural Fairness

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

59. 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 Industry 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

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

Key Definitions

61. **Industry 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.

62. **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

<table>
<thead>
<tr>
<th>DSPF Control</th>
<th>Defence Industry Security Program</th>
</tr>
</thead>
<tbody>
<tr>
<td>Control Owner</td>
<td>Assistant Secretary Security Policy and Services</td>
</tr>
<tr>
<td>DSPF Number</td>
<td>16.1</td>
</tr>
<tr>
<td>Version</td>
<td>1</td>
</tr>
<tr>
<td>Publication date</td>
<td>30 June 2018</td>
</tr>
<tr>
<td>Type of control</td>
<td>Enterprise</td>
</tr>
<tr>
<td>Releasable to</td>
<td>Defence and Defence Industry</td>
</tr>
<tr>
<td>General Principle and Expected Outcomes</td>
<td>Defence Industry Security Program</td>
</tr>
</tbody>
</table>
**Version control**

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

<table>
<thead>
<tr>
<th>Version</th>
<th>Date</th>
<th>Author</th>
<th>Description of changes</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Annex A

Defence Industry Security Program-Privacy Notice

Defence Industry Security Industry Program Privacy Notice

63. 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) 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, use and discloses personal information.

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

64. The DISP process undertakes a risk based assessment on your entities suitability to gain and maintain DISP membership. In order to process your DISP application and make a determination, DS&VS may share your personal information with:
   • Australian Security Intelligence Organisation (ASIO);
   • Australian Signals Directorate (ASD);
   • Relevant Defence groups and services;

The purpose for collecting your information

65. 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

66. 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.

67. 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

The Privacy Act 1998

Further information can be found at Defence Privacy Policy.
### Annex B

**Defence Industry Security Program - Suitability Matrix**

<table>
<thead>
<tr>
<th>Governance</th>
<th>Personnel Security</th>
<th>Physical Security</th>
<th>Information and Cyber Security</th>
</tr>
</thead>
</table>
| **Entry Level** | • Provide business details  
• Provide points of contact  
• Must have a nominated Chief Security Officer (must be able to meet AGSVA eligibility requirements for Baseline clearance)  
• Must have a nominated Security Officer (must be able to meet AGSVA eligibility requirements for Baseline clearance)  
• Security Officer must understand and effectively manage personnel/facilities and Information and cyber security up to an Unclassified/DLM level  
• Report changes in Foreign Ownership Control & Influence  
• Implement Security Policy & Plans  
• Insider threat program  
• Security Standing Orders  
• Risk assessment  
• Undertake training and awareness  
• Introduction to DISP course to be completed by SO  
• Annual Security Awareness Course – to be completed by all personnel  
• Reporting and management of security incidents and foreign contacts  
• Conduct travel briefings  
• Complete annual assurance activities  
• Protective Security Self-Assessment - no requirement for submission to Defence. May be subject to spot review by Defence upon request.  
• Maintain an appropriate system of risk oversight and management (i.e. risk register including security considerations) | • Security Officer 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 recruits | • Provide a description of physical security and access controls at each facility and their location | • Provide a description of information and cyber security practices and accreditations. For example:  
- Unclassified/DLM network in accordance with the ISM/DSPF  
- ISO/IEC 27011:2013 Information security management  
- ASD Essential 8  
- 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) |
| **Level 1** | All governance requirements from the Entry Level, plus:  
• Complete annual assurance activities  
  o Protective Security Self-Assessment submitted for Defence review  
• 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  
• Undertake training and awareness  
  o Security Officer course  
• Security officer may request Defence Online Security Dashboard (DOSD) access  
• Maintain a list of Designated Security Assessed Positions (DSAP) | All personnel requirements from the Entry Level, plus:  
• Security Officer has the ability to sponsor security clearances up to NV2  
• 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 ISM/DSPF to receive, handle, store and destroy PROTECTED information and material | • 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 NV2  
• 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 ISM/DSPF to receive, handle, store and destroy SECRET information and material | • 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 manages 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 NV/2/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 ISM/DSPF to receive, handle, store and destroy TOP SECRET information and material | • Ensure a TOP SECRET network or standalone device is employed in accordance with the ISM/DSPF |

*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.*
The exception to this is where industry may have accreditation recognised under an SIA. DISP membership is not required for the electronic storage and processing of PROTECTED information if the company is using Defence facilities and assets, including access to information on the Defence Network and DREAMS via laptop.

The Chief Security Officer must be a member of the organisation’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.

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 by the Operating Guide. If necessary, the Chief Security Officer, and Security Officer, may be the same individual.

We recommend a generic email address for example security@insertbusinessname.com, which can remain the same, rather than a personal email address.

Where the DSPF does not specify a policy position, industry should refer to the PSPF for guidance.

The CSO and SO can be the same individual.


See Principle 45 – Contact Reporting

PSSAs will be completed by DISP members at Entry level and may be subject to random spot checks.

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.

Also see Principle 23 – ICT Certification and Accreditation, and Principle 73 – Physical Security Certification and Accreditation.

Affected parties are those that are related to a contracted project or program.