Australian Government
Defence

FACTSHEET: REQUIREMENTS OF A DISP MEMBER

The Defence Industry Security Program (DISP) is governed by Principle 16 and Control 16.1 of the Defence Security Principles Framework (DSPF) including associated requirements contained within the broader DSPF, Protective Security Policy Framework (PSPF) and Information Security Manual (ISM).

Each authoritative document will be updated from time to time and it is the responsibility of the DISP member to ensure its security policies, procedures and processes are maintained and updated to meet the most current policy requirements.

ONGOING OBLIGATIONS OF DISP MEMBERS

Chief Security Officer (CSO) and Security Officer (SO)

Maintain the requisite security clearance for level of DISP membership[1].

Maintain SO Training Course completion every three years[2].

Monitor the DISP email address on a regular basis and respond to requests for information in a timely manner[3].

Annual Security Report

Submit the Annual Security Report (ASR) through the DISP Member Portal on the anniversary date of DISP membership being granted[4].

Ensure the ASR and any associated recommendations are agreed to by an Australian Board or Board equivalent, comprised of Australian citizens before submission to DISP[5].

Conduct security related assurance activities throughout the year to support ASR submission[6]. Activities could include, but are not limited to:

- Reconciliations of the Designated Security Assessed Positions (DSAP) against new starters list, leavers list and MyClearance records;
- Completion of overseas travel briefings and debriefs including AB644s;
- Completion of new starter briefings and exit debriefs in accordance with the new starter and leavers lists;
- Completion of Defence Annual Security Awareness training by all Defence engaged personnel within the past 12 months; and
- Maintaining the currency of the SPPs and validating annual acknowledgement by all Defence engaged personnel.

Sponsorship of Clearances

Sponsor security clearances in accordance with DSPF requirements, ensuring that:

- Clearance levels sponsored are in line with the DISP membership level held;
- DISP is a membership-based program that sets baseline security requirements for Industry Entities wishing to engage with defence[7];
- the CSO and/or SO sponsoring clearances hold a minimum of NV1 (Baseline clearance holders are unable to sponsor clearances)[8]; and
- clearances are not sponsored above the sponsor's own clearance level (e.g. NV1 cannot sponsor NV2)[9].

Withdraw sponsorship of clearances for staff that no longer need it; and, de-activate/re-activate clearances for clearance subjects between Defence engagements. See Managing an existing clearance | Australian Government Security Vetting Agency for more information.

Clearance sponsors are responsible for the management of clearance subjects and clearance holders including[10]:

- briefing clearance holders on their security responsibilities;
- managing individuals who have been granted a clearance with an eligibility waiver, in accordance with the provisions of the accompanying risk assessment or maintenance conditions;
- monitoring personnel behaviour and attitudes towards security;
- ensuring personnel participate in security awareness and training programs;
- reporting any security concerns to AGSVA; and
- ensuring that staff report any relevant changes in their personal circumstances to AGSVA.

CG: JUL026-26

Annual Security Awareness Training (ASAT)

All security cleared and Defence engaged personnel (including employees and contractors) are required to complete an endorsed Defence Annual Security Awareness Training (ASAT) course every 12 months. The DISP member must have mechanisms to monitor and maintain evidence of its completion.

The three endorsed training mechanisms include:

- Learn eXcel Perform (LXP);
- ADELE O:S; and
- SCORM package downloaded from the SO Portal.
- Entities may develop and facilitate their own ASAT training subject to the training being endorsed by the 'Security Culture, Uplift and Professionalisation' Branch.

Insider Threat Program

DISP members are required to maintain an Insider Threat Program proportionate to their size, operating environment, and risk profile.

At a minimum, the program should include:

- governance arrangements and accountability for insider threat management;
- awareness activities for security cleared and Defence engaged personnel;
- clear reporting and escalation pathways; and
- integration with personnel security, security incident reporting, and risk management processes.

Reportable Changes

A number of changes affecting membership are reportable to Defence including changes to[11]:

- CSO and/or SO within 14 days of the change;
- Ownership, including:
  - mergers and acquisitions;
  - organisational structure; and
  - controlling interest.
- key personnel (including senior executives and board members);
- financial position and financial viability;
- international supply chain activities;
- partnerships and joint ventures with foreign entities;
- significant business dealings with foreign entities;
- engagement of foreign nationals;
- exposure to criminal or other unlawful activities;
- any other activity or incident which may influence the Entity's ability to continue working with Defence;
- updates to physical locations, business name and DISP emails;
- change in contract requirements (including subcontracting arrangements and prime arrangements);
- major updates to network configuration; or
- if DISP membership is no longer required (request for withdrawal of membership).

A number of these changes can be submitted through the DISP Member Portal via a Change in Circumstance Report.

Security Incidents and Contact Reports

Security Incidents must be reported to Defence via an XP188 form within 24 hours of the incident occurring or becoming known, and recorded in the Security Register (tab F1)[12].

Supply Chain Management

Defence Industry is expected to manage security risks throughout the life cycle of a supplier arrangement including[13]:

- Security risk assessment of potential suppliers;
- Security controls to manage identified risks (e.g. flow through of Defence contract terms and conditions, contract terms to allow audit and verification activities);
- Contractual terms and conditions require potential suppliers to report any actual or suspected security incidents to the Defence Industry Entity; and
- Contract cessation / termination (e.g. clauses relating to destruction / return of Defence assets).

Ongoing Audit and Assurance

DISP members are required to participate in ongoing audit and assurance activities that includes, Ongoing Suitability Assessments (OSAs) and/or Deep Dive Audits (DDAs). DISP members are required to remediate recommendations within a mutually agreed timeframe[14].

Designated Security Assessed Positions (DSAP) Register

All Defence positions requiring a clearance must be recorded in the DSAP, along with the level of clearance required[15]. Where individuals are between Defence contracts, the SO should remove interest and reinstate it as needed via MyClearance[16].

Security clearance level requirements for Defence industry providers are determined by Defence capability managers and contract managers on the basis of their need to access Australian Government resources (people, information and assets)[17].

Where access to security classified resources is not required, some individuals may work in positions of high responsibility, or may have delegations and duties that, if mishandled or abused, could cause Defence considerable harm or reputational damage. Positions meeting this criterion should be identified as DSAP and the supporting rationale or risk assessment recorded in a DSAP register[18].

Physical Accreditation

Entities seeking to receive, hold or store physical Defence classified materials above OFFICIAL: Sensitive level will need the right level of physical accreditation from the Defence accreditation / certification body and meet all the physical security requirements of the ASIO Tech Notes[19]. Security Construction and Equipment Committee (SCEC) endorsement of the facility alone will be insufficient to hold Defence classified materials at PROTECTED level or above.

Protection of Defence Information

Defence Official information is all information received, developed or collected by, or on behalf of, the Australian Government by Defence personnel and persons engaged under a contract in their professional capacity[20].

All Defence information must be managed in accordance with its classification. More information on information classification, its removal, copying, disposal and transfer can be found in the DSPF Control 10.1 and the Assessing and Protecting Official Information Guide.

Release of Defence Official and Official: Sensitive materials must follow the requirements contained in DSPF Control 15.1.

DISP Cyber Scope

All DISP members are required to meet or exceed the Australian Signals Directorate's (ASD) Essential Eight (Essential 8)[21] at Maturity Level 2 across all of the Entity's ICT corporate systems[22] used to correspond with Defence[23].

Australian hosted DISP email

It is a requirement that all entities ensure their DISP email server is hosted within Australia.

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[24].

Data Sovereignty

Defence data is not stored or processed in jurisdictions where foreign governments have mechanisms to access information[25].

As a CSO or SO, you may request access to the DISP Security Portal, which can be accessed **here**[26]. The DISP Security Portal contains a number of useful references including the DSPF, other DISP related factsheets and SCORM packages for the Defence Annual Security Awareness Training. You will need an account created, which can be facilitated through emailing **DISP.info@defence.gov.au**.

For further information on the member responsibilities, refer to the **Maintaining Membership** page, or contact **DISP.info@defence.gov.au.**

ENDNOTES

1 DSPF Control 16.1 para 62; para 69; para 70.
2 DSPF Control 16.1 para 65; para 71.
3 DSPF Control 16.1 para 22.
4 DSPF Control 16.1 para 69 a.
5 DSPF Control 16.1 para 66 e.
6 DSPF Control 16.1 Annex A.
7 DSPF Control 40.1 para 113.
8 DSPF Control 16.1 para 70.
9 Ibid.
10 DSPF Control 40.1 para 143 h.
11 DSPF Control 16.1 para 35; para 66 f; para 67; Annex A.
12 DSPF Control 16.1 para 34 b; para 71 e; Annex A; Control 77.1.
13 PSPF Policy 6 Requirement 39-42.
14 DSPF Control 16.1 para 36 b and c; para 37 and 38; para 61 f.
15 DSPF Control 40.1 para 104.
16 DSPF Control 16.1 Annex A.
17 DSPF Control 40.1 para 113.
18 DSPF Control 40.1 para 107.
19 ASIO Technical Note 1/15 - Physical Security of Zones (Zones 2 - 4)
20 DSPF Control 15.1 para 3. A.
21 Essential Eight assessment process guide.
22 PSPF Control 13.2 - Technology Estate.
23 DSPF Control 16.1 Annex A.
24 DSPF Control 16.1 para 22.
25 Control 27.1 para 6 e; *Privacy Act 1988* - Federal Register of Legislation - Part 3, Division 1, Paragraph 13; Control 15.1 Annex B Appendix 1; PFPS 12.3.1.
26 Note the DISP Security Portal is different to the DISP Member Portal, which should be used to manage ongoing reporting requirements of DISP members.

To defend Australia and its national interests in order to advance Australia's security and prosperity
www.defence.gov.au

CG: JUL026-26