

Policy Factsheet

## Changes to DSPF Principle 16 and Control 16.1

Overview

Defence has updated and uplifted the security controls that govern the Defence Industry Security Program (DISP) in the Defence Security Principles Framework (Principle 16 and Control 16.1). These changes have been made to strengthen industry security standards and align the policy with new processes ahead of the DISP Membership System Change Release 2 on 30 September 2024.

Key Changes

Key changes made to DSPF Principle 16 and Control 16.1 include:

1. Updating outdated language (e.g. references to DISO).
2. Replacing references to DISP membership forms (AE250 – DISP Application, AE250-1 – FOCI and AE250-2 – Notification of Engagement Requiring DISP Membership) with hyperlinks to the [DISP Member Portal](https://www.defence.gov.au/business-industry/industry-governance/industry-regulators/defence-industry-security-program/resources/disp-member-portal) and [Notification of Engagement Requiring DISP Membership](file:///C:\Users\hollie.zuber\Objective\Objects\Notification%20of%20Engagement%20Requiring%20DISP%20Membership%20Portal) link.
   1. The AE250 and AE250-1 forms can still be used for membership upgrades. New applications must use the DISP Member Portal.
   2. The AE250-2 form should only be used by Contract Managers where there is a need to include classified information above PROTECTED on the engagement requiring DISP membership. For all other engagements use the Notification of Engagement Requiring DISP Membership link.
3. A mandatory provision for Industry Entities who are Australian Community Members pursuant to the Australia-US Defence Trade Cooperation Treaty to hold DISP membership (paragraph 5.d).
   1. It is already a requirement of the Treaty that Australian Community Members hold DISP membership; the requirement has been reinforced in policy.
   2. Further information on the Treaty can be found [here](https://www.defence.gov.au/business-industry/exporting/us-trade-treaty). DISP members can contact [dec.outreach@defence.gov.au](mailto:dec.outreach@defence.gov.au), if they have questions specific to their obligations under the Treaty.
4. An additional Annex (Annex C – Special Access Programs) setting out supplementary requirements for DISP members participating in Special Access Programs (SAP). SAP manage Defence’s most sensitive capabilities and information. The additional requirements in Annex C ensure that Defence’s most sensitive information is appropriately protected. DISP members participating in SAP must:
   1. Hold DISP Level 3 membership in the Governance and Personnel Security domains;
   2. Agree to apply the security controls outlined in the SAP Manual (SAPMAN); and
   3. Apply any additional security measures required by Defence’s Chief Security Officer.
5. Information on where DISP email systems can be hosted and the format for primary contact email addresses (paragraph 22).
   1. The format must be: DISP@company domain name. Web-based mail services such as Google, Yahoo, AOL, Yandex etc. will not be accepted.
   2. DISP will accept variations such as .com.au, .com, .biz, or .net, however email systems used for DISP membership must be hosted in Australia.
6. Clarity on Chief Security Officer (CSO) Personnel Security Clearances (PSC) and training requirements.
   1. An Industry Entity’s CSO must be able to obtain and maintain a PSC commensurate with the Industry Entity’s level of DISP membership (this means if an entity applies for Level 3 membership, the CSO must have an NV2 PSC) (paragraph 62).
   2. The CSO is required to complete the DISP Security Officer Training course as part of the application process, and every three years thereafter (paragraph 65).
7. Further information on Security Officer PSC requirements for Level 3 DISP members, and PSC requirements for SOs sponsoring PSCs.
   1. Where an Industry Entity holds Level 3 DISP membership, SOs with limited security responsibilities may hold lower level PSCs. Industry Entities must document in their security policies and plans the roles and responsibilities of SOs that hold lower level PSCs (paragraph 69).
   2. SOs cannot sponsor PSCs at a higher level than the PSC level they hold (e.g. an NV1 clearance holder cannot sponsor NV2 clearances) (paragraph 70).
8. Minimum cyber security requirements for DISP members will be upgraded from the Australian Signals Directorate’s (ASD) Top 4 to ASD’s Essential Eight (Annex A, Entry level ICT & Cyber Security domain).
   1. This change has been made to ensure that DISP members’ cyber security controls remain effective in mitigating cyber security attacks. DISP members can find further information on the changes on the DISP [website](https://www.defence.gov.au/business-industry/industry-governance/industry-regulators/defence-industry-security-program/cyber-assurance).

For further information on the changes, refer to the Defence Security Principles Framework in the Resources tab on the DISP [website](https://www.defence.gov.au/business-industry/industry-governance/industry-regulators/defence-industry-security-program/resources), or contact [DISP.info@defence.gov.au](mailto:DISP.info@defence.gov.au).