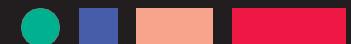




Defence Industry
Security Program

Defence Industry Security Program

May 2019





Security Environment

- Corporate Espionage
- Foreign Espionage and Interference
- Foreign Ownership, Control and Influence
- Cyber threats
- Insider threats
- Variable security culture/focus in industry
- Global supply chains
- Changing workforce demographics





Old DISP



- Membership was contract-based
- Multiple memberships per company
- Identified barriers to participation
- Review, consultation and pilot process



DISP Reforms

Benefits for Industry



- Open membership
- Streamlined access to security services
- Flexible DISP membership levels
- Sponsor staff security clearances*



Benefits for Defence



- Strengthened security requirements and reporting
- Minimum cyber security standards
- Integration into the Smart Buyer Framework
- Updated contracting clauses





Membership Categories

Governance

Must match highest level of membership sought for any other category

Personnel Security

Physical Security

Information & Cyber Security

Entry Level



- CSO & SO (Baseline cleared)
- Security policy and plans
- Insider threat program
- Assurance reporting

- Employment screening of personnel (AS4811-2006)

- My business requires rooms/facilities able to store UNCLASSIFIED/DLM information (self certification or accreditation)

- My business ICT network does not process or store any classified information
- Business is required to meet UNCLASSIFIED/DLM ICT network self accreditation

Level 1



- All requirements from Entry level plus
- SO must understand and effectively manage personnel, facilities and information/cyber security up to PROTECTED.

- My business requires employees to have Baseline security clearances
- My Business can sponsor security clearances¹

- My business requires rooms/facilities accredited to store PROTECTED information or assets

- My business ICT networks require accreditation to handle PROTECTED information

Level 2



- All requirements from level 1 plus
- SO must understand and effectively manage personnel, facilities and information/cyber security up to SECRET.

- My business requires employees to have NV1 security clearances

- My business requires rooms/facilities accredited to store SECRET information or assets

- My business ICT networks require accreditation to handle SECRET information

Level 3*



- All requirements from Level 2 plus
- SO must understand and effectively manage personnel, facilities and information/cyber security up to TOP SECRET.

- My business requires employees to have NV2/PV security clearances²

- My business requires rooms/facilities accredited to store TOP SECRET information or assets

- My business ICT networks require accreditation to handle TOP SECRET information

Defence Industry Security Office (DISO)



Conduct security assurance and audit activities across DISP



Provide security support and advice to industry



Increase industry engagement with other Departments and agencies



Membership Costs

- No membership fees
- Indirect costs associated with applying for and maintaining DISP membership
 - Security clearances (vetting fees available on AGSVA's website)
 - Time and travel to attend training
 - Implementing governance, personnel, physical and information/cyber security requirements

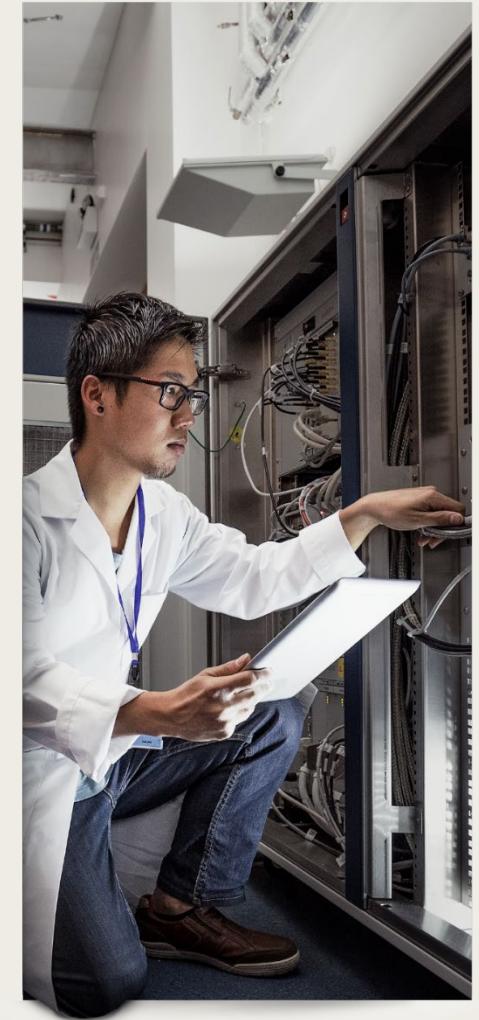
Governance

- ✓ Chief Security Officer – responsible for appropriate systems of risk oversight and management
- ✓ Security Officer – responsible for the day-to-day security risk management
- ✓ Foreign Ownership Control & Influence (FOCI)
- ✓ Business Risk Assessment
- ✓ Security Policies and Plans
- ✓ Annual Security Awareness Training - Insider Threat Program
- ✓ Reporting (Annual Security Report, Incidents, Foreign Contacts)



Personnel Security

- ✓ Australian Employment Screening Standards 4811 – 2006
- ✓ AS4811 – 2006 is under review with broadened scope to cover
 - ✓ Ongoing Suitability
 - ✓ Separation
- ✓ Important to understand your workforce to be able to implement physical and information/cyber access controls





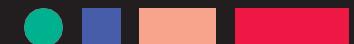
Physical Security

Entry Level

- Provide a description of physical security and access controls at each facility and location

Level 1 – Level 3

- Certified and accredited in accordance with the DSPF to store and handle appropriate level of classified material



Information & Cyber Security

- ✓ ISO/IEC 27001/2:2013
- ✓ NIST SP 800-171 (US ITAR requirement)
- ✓ Cyber security for defence suppliers (Def Stan 05-138)
- ✓ Unclassified/DLM Network in accordance with the ISM/DSPF
- ✓ Following requirements of ASD Essential 8
 - Restrict administrative privileges
 - Application whitelisting
 - Patch applications
 - Patch operating systems

Extant DISP Members

- Up to 24 month timeframe to transition
 - Can transition earlier at a time of their choosing or
 - As a new contractual requirement
- Required to submit a new DISP application
 - Where applicable, DS&VS will consolidate multiple memberships into a single membership





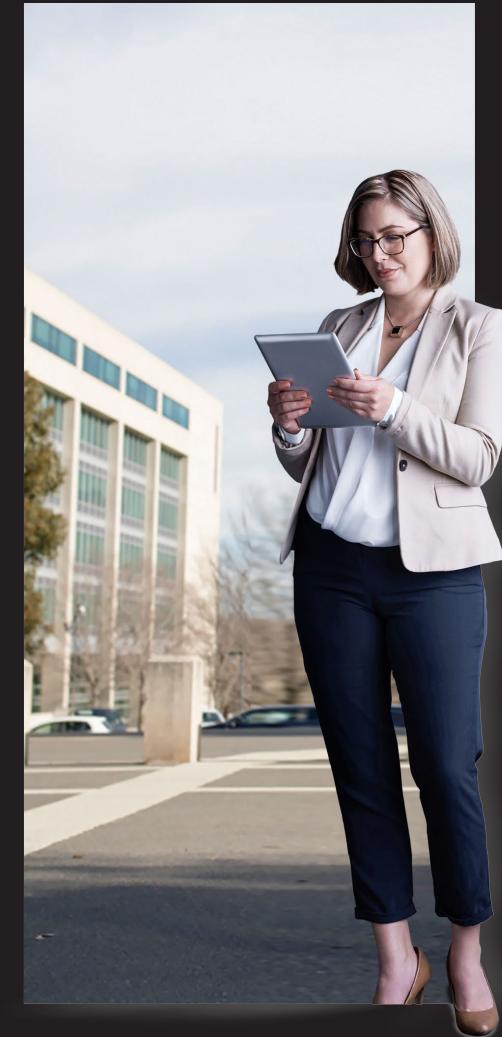
How to Apply

- ✓ Visit DISP website – Search DISP
- ✓ Submit DISP Application (AE250)
- and
- ✓ Submit Foreign Ownership Control and Influence (FOCI) (AE250-1)

The screenshot shows the homepage of the DISP website. At the top, the Australian Government Department of Defence logo is displayed, followed by the text "Defence Security and Vetting Service" and "Enabling Defence capability through security services". Below this is a navigation bar with links: "Department of Defence", "Defence Security and Vetting Service", "Industry Security Program", and "Home". The main content area has a sidebar titled "DS&VS" with links to "Home", "Roles And Responsibilities", "Careers", "Industry", and "Defence Security Principles Framework". A "Contact Us" section provides information for vetting and clearance enquiries, directing them to the "Australian Government Security Vetting Agency". Another section for general security enquiries provides contact details for the Defence Service Centre. The main content area features a heading "Welcome to Defence Industry Security Program (DISP)" and text explaining the reformation of DISP to provide industry increased opportunities to work with Defence and easier access to Defence security services. It also mentions that industry can self-nominate for DISP membership without a Defence contract, which supports industry to become Defence-ready. A video player is shown with the text "Watch the videos below to find out more: Welcome to DISP" and "Changes to DISP". The bottom of the page features a decorative footer with colored squares (green, blue, orange, red) and the text "We've simplified how you become a member".

Contract Manager's Obligations

- Manage Project risks
- Check DISP membership levels
- Notification of Contract/Panel/Partnership webform (AE250-2)
- Ensure appropriate security clauses are included in contracts/written agreements
- Ensure additional project-specific security requirements are resourced and managed





DISP.info@defence.gov.au

www.defence.gov.au/dsvs/industry