Defence Security and DISP

This is a 4-hour face to face course covering critical information needed to secure your Defence Industry business in "the most challenging geopolitical circumstances since the Second World War". It covers an understanding of new security requirements for working with Australian Defence and Defence Industry Primes, explores the capabilities required for Defence Industry Security Program (DISP) membership, enables detailed understanding of cybersecurity requirements and good practice for Defence Industry, then introduces other security factors and different requirements for working with AUKUS partners and globally.

This Practitioner level course covers intermediate level knowledge of current Defence and Defence Industry Security and Cybersecurity.

The course has been designed for a broad mix of roles, from security officers to department and project managers in the Defence Industry. **BRING A LAPTOP OR TABLET TO THE SESSION TO PARTICIPATE IN THE COURSE ACTIVITES.**

Course Cost

AIDN Members – Free (multiple attendees) Non-AIDN Members $400.00 ex GST (per attendee)

Course Curriculum

Section 1 (1 hour) – Defence Security Requirements

- Defence and Defence Industry Security Overview: What Are Defence's Priorities
- Defence and Primes security requirements - Supply chain risk management
- Security Stakeholders and Obligations, Defence, Government, Law and Contractual
- Threat Environment and Actors International Environment
- Data Sovereignty and Handling Defence Information, Cloud and Classif Classifications
- International Security Requirements

Section 2 (1 hour) – Defence Industry Security Program (DISP)

- Overview of DISP and Membership Levels
- Governance – What appointments and internal processes
- Personnel – Clearances Australian Government and export control considerations
- Physical – Entry Level, Physical Security Zones, export control considerations
- Application Process and Overview
- Ongoing Suitability Assessments – basic, deep dive and what to expect
- Recent changes – ICT and Cyber, Annual Security Reports

Section 3 (1 hour) – ICT Security Key Concepts

- Security Technology Basic: Identity and Access Management, Multi-Factor Authentication, Vulnerability Management, and Backups
- Technology Investments Advanced: Application Control, Logging and Monitoring (SIEM), Managed Detection and Response, and Document Loss Protection.
- Classified Environments

Section 4 (1 hour) – Other Security Factors

- Security Technology Basic: Identity and Access Management, Multi-Factor Authentication, Vulnerability Management, and Backups
- Australian vs International Security Standards: Differences, Similarities and using together
- Security of Information Agreements: Overview and applicability
- Defence Primes Security Programs: JOSCAR, Supply Chain Security Assessments
- US Market – Cybersecurity Maturity Model Certification (CMMC)
- International Traffic in Arms Regulations (ITAR) Security considerations and implications
- AUKUS – Security requirements and changes
- Security Grants: criteria and implications
- Putting it all together – managing your security.

Assessment

- Digitally Administered Theory Exam
- Attendee Feedback Survey