



Australian Government

Defence



DISP

Membership Program

Defence Industry Security Program



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



Contents

What is DISP?	2	Cyber Security Uplift	8
DISP Security Domains	4	DISP Membership Portal	10
Detailed DISP Membership process	5	How to apply	11
DISP Compliance and Assurance	6	Security Training Resources	12

Foreword

Welcome to the Defence Industry Security Program, a security assurance service for Australian businesses and other entities wishing to partner with Defence.

This brochure provides an overview of the Program – commonly referred to as DISP – and its mission of ensuring industry has the right security in place for Defence tenders and contracts, and Defence capabilities are underpinned by a strong security culture and secure workforce.

PROTECTING WHAT'S IMPORTANT

Major power competition, military modernisation, foreign interference and disruptive technology threats are all making our region less safe.

As the environment changes around us, Defence joins other Government agencies in uplifting the security of Australia's critical infrastructure and the essential services that underpin our prosperity and way of life – this includes the security of defence industry and its supply chains.

The Defence Industry Development Strategy 2024 establishes the framework and principles for Australia's Defence industry policy and provides a roadmap for supporting our industrial base to deliver uncompromised capability.

The Strategy seeks to deliver a number of initiatives required to develop Australia's sovereign Defence industrial base and meet Australia's national security requirements.

In support of this initiative, we remind defence industry that a dedicated security grant has been established to support small to medium businesses to uplift and maintain their security posture. Grant values range from between \$10,000 and \$100,000 and are available over the next 4 years.

DISP MEMBERSHIP

DISP is rapidly expanding to meet the demands of a number of initiatives being driven by the Government, including AUKUS. We currently have over 1400 accredited members and expect to grow to 2000 members during 2025.

If you are new to DISP – or you're seeking to upgrade your membership – I urge you to review the application process thoroughly to ensure your request is processed in the shortest possible timeframe. The threats to Defence industry are real, and DISP processes, timeframes and assurance reflect the seriousness of those threats.

Thank you for taking the time to learn more about DISP. I look forward to working with you in building a more secure defence industry.

Kate Dann

Assistant Secretary, Defence Industry Security

What is DISP?

The Defence Industry Security Program, managed by the Defence Industry Security Branch, is a multi-level membership based program underpinned by the Defence Security Principles Framework - Principle 16, Control 16.1.

Its purpose is to:

- › Ensure industry has the right security in place for Defence tenders and contracts.
- › Provide industry with access to security advice and support services.
- › Help industry to understand and manage security risks.
- › Provide confidence and assurance to Defence and other government entities when procuring goods and services from industry members.

COST

There is no direct cost associated with DISP membership, i.e. there is no membership fee.

However, there are costs associated with implementing and maintaining security measures to meet both initial and ongoing DISP membership requirements.

These might include facility certification and accreditation, personnel security clearances, cyber security uplift and physical security measures.

WHO CAN APPLY?

DISP membership is open to any Australian entities (with an ABN or ACN) looking to become part of the Defence industry supply chain.

WHO SHOULD APPLY?

DISP membership is open to Australian entities looking to become part of the Defence industry supply chain. To become a DISP member an industry entity needs to meet base eligibility criteria. There are also additional criteria based on the level of membership required.

Depending on the type of work an entity undertakes with Defence, or any contractual requirements, DISP membership may be mandated. Membership is not mandated in all circumstances. However, it is highly recommended for any entity currently working on Defence projects or for those seeking to partner with Defence.

! IMPORTANT

DISP membership is not automatic. Entities must demonstrate they have met the security standards for the levels they have nominated. They must also meet suitability considerations, such as Foreign Ownership, Control and Influences assessments conducted by Defence.

DISP MEMBERSHIP BENEFITS

Membership to DISP provides entities with:

- › Access to Defence security services that will enable an entity to be Defence-ready.
- › Ability to sponsor security clearances (note not available for entry level membership).
- › Access to security training and materials, including cyber security guidance.
- › Access to current security information to assist in security practices and planning.
- › Improved security operating environment as security practices are strengthened.

DISP membership does not guarantee Defence contracts for entities. These are still subject to the usual procurement processes.

DISP MEMBERSHIP TIMEFRAMES

The timeframe between submitting an application and receiving DISP membership will vary with each entity and depend upon:

- › The level of membership being sought
- › Priority of Defence work to be undertaken by the entity
- › The suitability of the entity
- › Level of preparedness undertaken by applicants

Generally, an application can take 90-180 days to complete depending on the conditions listed above.

What is DISP?

DISP MEMBERSHIP LEVELS

DISP has four membership levels within each security domain:

➔ Entry	Official / Official: Sensitive
1 One	Protected
2 Two	Secret
3 Three	Top Secret

These levels reflect the security obligations that align with the Australian Classification System, applicants can self-nominate the membership levels they wish to apply for. Nominations must reflect the level of security required to meet current and/or likely Defence security obligations. Membership levels 1-3 require a supporting business case.

UPGRADING DISP MEMBERSHIPS

Entities that are entering new contracts, tenders or projects, may require a higher membership level.

The Defence Security Principles Framework (DSPF) can assist in determining what level of membership is required based on business needs or contractual requirements.

Please email disp.info@defence.gov.au if you need information on how to upgrade membership levels.

DISP MEMBER RESPONSIBILITIES

DISP membership comes with ongoing responsibilities at every level.

These are set out in Control 16.1 in the DSPF. These include but are not limited to:

- › The safeguard of Defence and industry's people, information and assets.
- › Appointing and retaining a CSO and SO.
- › Reporting changes that may affect DISP membership.
- › Submitting an Annual Security Report (ASR) every 12 months from the start date of DISP membership.
- › Regular security training of staff including induction training.
- › Ongoing employment screening and suitability checks.
- › Maintaining a classified document register if accessing information at Official Sensitive or higher.
- › Adhering to mandatory requirements regarding personnel access to Defence buildings and systems.

In the event of any security incidents, submit an XP188 Security Report form and notify your Security Officer.

The Security Incident Coordination Centre will ensure the security incident is effectively managed. In accordance with DSPF Control 77.1, persons engaged under a contract must also report the incident to their contract manager.

The first military combat aircraft to be designed, engineered and manufactured in Australia in more than 50 years, the MQ-28A Ghost Bat is an autonomous air vehicle intended to operate as part of an integrated system of crewed and un-crewed aircraft and space-based capabilities



DISP Security Domains

DISP membership requirements are articulated across four security domains. These security pillars provide the foundation to safeguard you, your company or business and the integrity of Defence's information, assets and people.



SECURITY GOVERNANCE

Security governance refers to an entity's accountability and responsibility for ensuring suitable plans, processes and people are in place to maintain the relevant levels of security.

It is having appropriate practices across physical security, personnel security, information and cyber security. This includes appropriate security education and training, and security incident response and reporting.

Security governance reflects an entity's ability to safeguard people, information and assets. There are a number of specific documents required to support the entity's DISP application.

Ongoing security governance obligations for DISP membership also include regular reporting documents that are self-managed and submitted for ongoing membership management.



PHYSICAL SECURITY

Physical security is the protection of people, property, and physical assets from actions and events that could result in damage or loss.

A secure physical environment helps to prevent or mitigate threats or attacks against Defence facilities, personnel, security protected information and assets. Physical security establishes the environment threat actors must work in, and is a building block of effective insider threat management and cyber security.

Physical security measures and procedures are continuously evolving as new threats emerge.

DISP membership requirements for physical security will depend on the level of security classification required for the receipt, handling, storage and destruction of information or physical assets that are being held at the facilities.



PERSONNEL SECURITY

Personnel security encompasses the suitability of an entity's employees and contractors to access government information and assets. This involves ensuring personnel have an appropriate standard of security competence, integrity and honesty.

Employment screening applies to security cleared and non-security cleared personnel, contractors and others who will have access to Australian Government resources.

DISP members need to meet Australian Standard for Workforce Screening AS 4811:2022 standard.

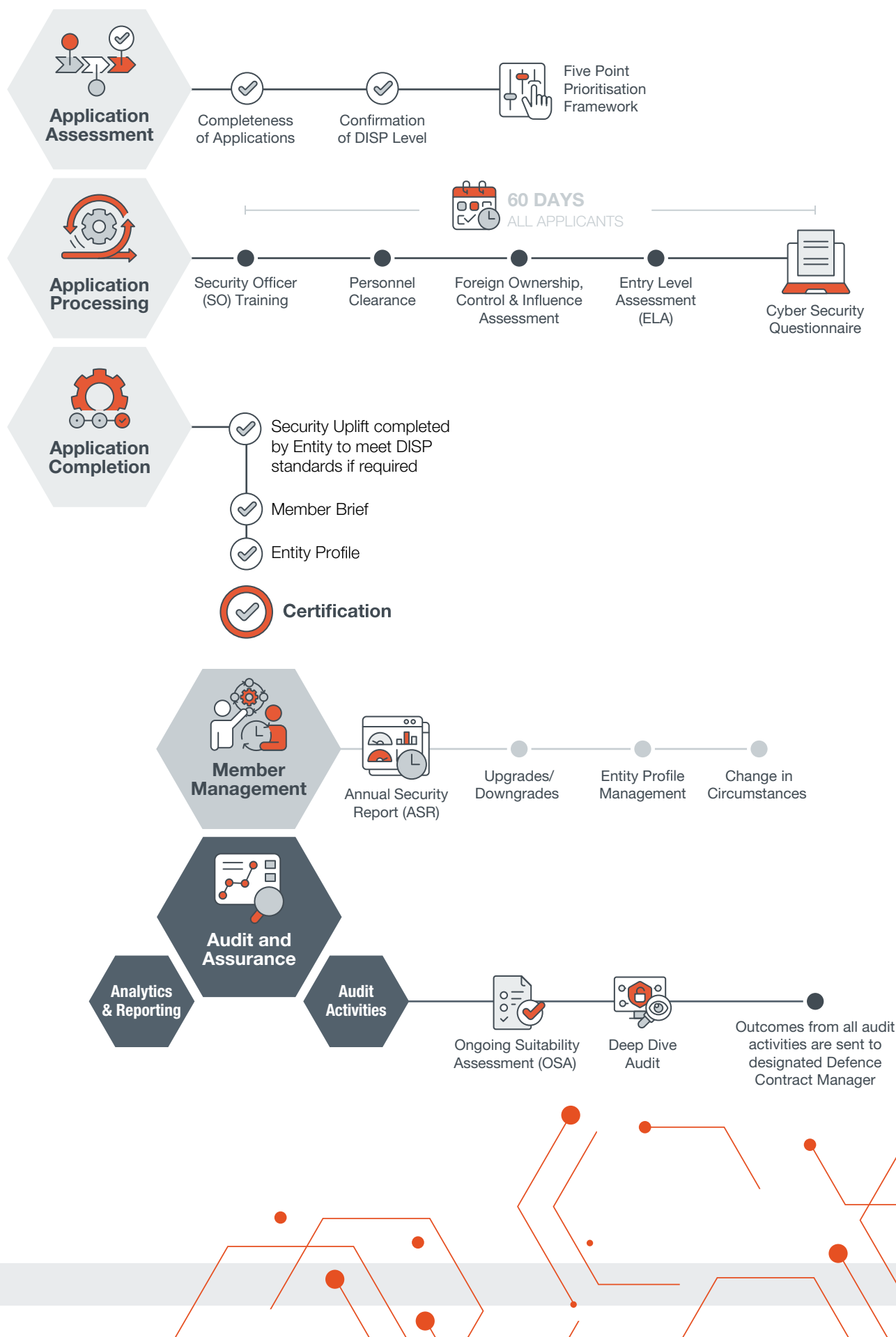


INFORMATION AND CYBER SECURITY

The Information and Cyber Security domain relates to the protection of Defence Official Information. DISP members may hold on their corporate system while ensuring appropriate security controls are in place.

To meet the Information and Cyber Security DISP membership requirements, an entity will need to demonstrate how they meet or exceed the Australian Signals Directorate (ASD) Essential Eight (E8) Mitigation Strategies at Maturity Level 2 across its ICT systems used to correspond with Defence.

Detailed DISP Membership Process



DISP Compliance and Assurance

DISP is underpinned by an assurance framework to ensure members maintain an appropriate security posture.

Where a DISP member demonstrates persistent disregard for DISP requirements or fails to undertake agreed corrective actions, Defence has scalable response options including downgrading, suspending or terminating their DISP membership – all impacting their ability to work with Defence and its supply chains.

Layered Assurance measures include:

ANNUAL SECURITY REPORTS



An Annual Security Report (ASR) is a self-attestation, completed by DISP members, of compliance with security obligations under DSPF which is due on the anniversary of the DISP membership certificate. An ASR is required to be tabled with the entity's Board or Executive (or other equivalent Governance forum) prior to submission to DISP, to ensure that appropriate Executive oversight and action is taken in response to any security issues identified.

DISP members may be required to provide additional information to DISP regarding the ASR responses provided.

ASRs are submitted through the DISP Member Portal.

ONGOING SUITABILITY ASSESSMENTS



An Ongoing Suitability Assessment (OSA) is a desktop audit to ensure that members are continuing to meet Defence security obligations. OSA selection is an outcome of an internal risk-based framework. An OSA will assess DISP member's compliance with a selection of security requirements across all 4 DISP security domains.

The OSA process includes a review of security documentation, a phone interview with security staff and the completion of a cyber-questionnaire. This activity assists DISP members to review, and where needed, improve their security policies, procedures, and risk management.

DEEP DIVE AUDITS



The DISP approach to deep dive audit (DDA) is one of collaboration.

The objective of a DDA is to ascertain the extent of DISP members' compliance with requirements of DSPF Control 16.1 through a detailed assessment (including site visits) of the adequacy of Defence security processes and controls in place, and if needed help to uplift an entities security posture. DISP members are selected for inclusion in a DDA based on an internal risk-based selection framework.

All identified security uplift activities or opportunities for improvement are discussed, and a draft report for review and comment is provided prior to being finalised. The implementation of all DDA recommendations is monitored by the DISP audit team.

CYBER SECURITY QUESTIONNAIRE



To meet DISP membership requirements, an entity must comply with the E8 at ML2, which is derived from the the Australian Government Information Security Manual.

To complete the Cyber Security Questionnaire (CSQ), provide comprehensive responses and evidence to the questions in the DISP E8 CSQ. It is recommended the CSQ be completed by an authorised representative who has sufficient knowledge of your/the organisation's corporate IT infrastructure. Incomplete answers or insufficient information will delay the application.

Within the CSQ, the 'Tool Tips' features relevant information on control implementation and acceptable evidence (in accordance with ASD's guidance).

Components of the F9 pistol, the ADFs newest sidearm which is offering personnel a reliable and efficient option for self-defence and combat situations. The rollout of the F9 pistol is set to continue throughout 2025.



Cyber Security Uplift

Malicious cyber activity continues to pose a risk to Australia's security and prosperity. The Cyber Security Questionnaire through the ASR has been uplifted to encompass the full Essential Eight (E8). This will increase the cyber hygiene and resilience for DISP Members.

DISP will provide a maturity action plan for E8 uplift when required. There are grants available to help SME DISP members cover expenses required to become compliant with E8.

E8 – NOVEMBER 2023

ASD has developed prioritised mitigation strategies to assist organisations mitigate cyber security incidents caused by various cyber threats.

The most effective of the mitigation strategies are the E8, which outlines a minimum set of preventative measures at graduated levels of maturity.

The DISP cyber standards are uplifting to assess against all the Mitigation Strategies that constitute the E8 at **Maturity Level 2 (ML2)**, including:

1. Application control
2. Patch applications
3. Configure Microsoft Office macro settings
4. User application hardening
5. Restrict administrative privileges
6. Patch operating systems
7. Multi-factor authentication
8. Regular backups.

Under the 2023 version at ML2, there are 107 security controls to be assessed.

An artist's impression of the BAE Systems SEA 5000 Future Frigate, Global Combat Ship - Australia.

Image credit: BAE Systems



E8 MITIGATION STRATEGIES

MITIGATION STRATEGY	WHAT	WHY
Application control	Checking programs against a pre-defined approved list and blocking all programs not on this list.	Unapproved programs including malware are unable to start and preventing attackers from running programs which enable them to gain access or steal data.
Patch applications	Apply security fixes/patches or mitigations (temporary workarounds) for programs within a timely manner (48 Hours for internet reachable applications). Do not use applications which are out-of-support and do not receive security fixes.	Unpatched applications can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems.
Restrict Microsoft Office Macros	Only allow Office macros (automated commands) where there is a business requirement and restrict the type of commands a macro can execute. Also monitor usage of Macros.	Macros can be used to run automated malicious commands that could let an attacker download and install malware.
User application hardening	Configure key programs (web browsers, office, PDF software, etc.) to apply settings that will make it more difficult for an attacker to successfully run commands to install malware.	Default settings on key programs like web browsers may not be the most secure configuration. Making changes will help reduce the ability of a compromised/malicious website from successfully downloading and installing malware.
Restrict administrative privileges	Limit how accounts with the ability to administer and alter key system and security settings can be accessed and used.	Administrator accounts are 'the keys to the kingdom' and so controlling their use will make it more difficult for an attacker to identify and successfully gain access to one of these accounts which would give them significant control over systems.
Patch operating systems	Apply security fixes/patches or temporary workarounds/mitigations for operating systems (e.g. Windows) within a timely manner (48 Hours for internet reachable applications). Do not use versions of an Operating system which are old and/or not receiving security fixes.	Unpatched operating systems can be exploited by attackers and in the worst case enable an attacker to completely takeover an application, access all information contained within and use this access to access connected systems.
Multi-factor authentication	A method of validating the user logging in by using additional checks separate to a password such as a code from an SMS/Mobile application or fingerprint scan.	Makes it significantly more difficult for adversaries to use stolen user credentials to facilitate further malicious activities.
Regular backups	Regular backups of important new or changed data, software and configuration settings, stored disconnected and retained for at least three months. Test the restoration process when the backup capability is initially implemented, annually and whenever IT infrastructure changes.	To ensure information can be accessed following a cyber-security incident e.g. a ransom-ware attack.

DISP Membership Portal


The DISP Membership Portal was launched on 6 December 2023 to streamline the DISP application process and improve Defence processing capabilities. DISP applicants can use the Portal to complete and lodge membership applications online.

Iterative releases are enabling self-service functionality for DISP members through The Portal. DISP members can complete their Annual Security Report (ASR) and Change in Circumstances (CiC) through the Portal from Q4 2024.

WHAT DOES THIS MEAN FOR DISP MEMBERS?

Self-service functionality improves user experience for DISP members engaging with Defence contracts.

Membership data will be more secure, accurate and accessible. Digital data captured via The Portal enables more efficient application processing by our DISP Membership team.



An Australian Army Hawkei protected mobility vehicle is prepared to be loaded onto a Royal Australian Air Force C-17A Globemaster III aircraft.

The Hawkei is an Australian-designed and manufactured vehicle built in Bendigo, Victoria, by Thales Australia.

How to apply

STEP 1

Familiarise yourself with Defence Security Principles Framework (DSPF), Australian Government security clearances and the Defence Industry Security Program (DISP) membership level requirements.

STEP 2

Determine the level of membership and assess how closely your business currently meets the levels of membership you require.

STEP 3

Head to the DISP Member Portal and fill out the application. The DISP membership team will then triage the application.



Security Training Resources

The following courses are available through the Adele Platform which can be accessed with the enrolment key you are provided throughout the DISP accreditation process. DISP Members are also able to download the Annual Security Awareness Course and the Assessing and Protecting Official Information Course training packages from the DISP Security Officer Portal (DOSD) for incorporation in their own training systems. The below courses will help support your journey as a Chief Security Officer and/or Security Officer.

ANNUAL SECURITY AWARENESS COURSE

DISP Members are required to contact DISP.info@defence.gov.au for the course enrolment instructions.

- Understand the nature and extent of the threats facing Defence.
- Understand the nature and extent of activities by trusted insiders.
- Understand the actions you can take to reduce the likelihood of being targeted in your personal life.
- Understand your ongoing personal obligations to protect Defence's people, information and assets.
- Know where to go for further security knowledge and advice.

ASSESSING AND PROTECTING OFFICIAL INFORMATION COURSE

DISP Members are required to contact DISP.info@defence.gov.au for the course enrolment instructions.

- Understand the importance of your role in protecting Official Information.
- Understanding policy and legislation associated with handling official information.
- Understand how to assess and protectively mark Official Information.
- Understand basic handling requirements (storage, transport, registration and disposal) of Official Information.
- Know where to find the Guide to Assessing and Protecting Official Information.
- This guide will provide you all your official information assessment and protection guidance whenever you require it.

SECURITY OFFICER COURSE

DISP Members are required to contact DISP.info@defence.gov.au for the course enrolment instructions.

- To provide security advice to command/management and colleagues.
- To provide support to command/management in their implementation of DSPF principles, processes and controls.
- To undertake basic Security Officer administrative tasks.
- To find templates/tools/forms/awareness products and further information to assist them back in the workplace.

SECURITY RISK MANAGEMENT WORKSHOP

- Understand their decision-making processes and those of others.
- Holistically understand the process of Security Risk Management.
- Articulate and create the individual considerations of Security Risk Management including Threat and Vulnerability Assessments.
- Understand how a SRA is created and how to begin managing residual risks through the DSPF.
- Be equipped with further resources, tools and templates.

**General Enquiries**

1800 DEFENCE (1800 333 362)
DISP.info@defence.gov.au

Engagement Enquiries

DISP.outreach@defence.gov.au

Useful Resources

www.defence.gov.au/security/industry/resources

Australian Government Security Vetting Agency (AGSVA)

securityclearances@defence.gov.au | 1800 640 450
www.agsva.gov.au

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

