DISP Security Awareness

Australian Government
Department of Defence

Defence Industry Security Program

Overview

The Defence Industry Security Program (DISP) assists in securing Defence capability through strengthened security practices in partnership with industry, and enhances Defence's ability to manage risk in the evolving security environment.

By placing a high personal value on security, you set the benchmark to foster a strong culture.

This introduction to security awareness will provide you with the overarching view of key security considerations, roles and approaches to help you become Defence-ready.

Security is everyone’s business

No matter what position you hold, everyone plays an integral role in maintaining your and Defence's security.

Security can be represented by primary five categories. Each play a role in providing a secure environment to guard against a range of threats and risk.

Having good awareness and practices in place for each greatly enhances your ability to protect what's important and enable you to be Defence-ready.

Key Security Roles: Defence Security and Vetting Service (DS&VS)

DS&VS is the protective security authority for Defence. It provides a number of products and services to Defence to ensure that security is properly addressed.

DS&VS responsibilities include:

- Security intelligence (such as Security Threat Likelihood Assessments)
- Defence Security Threat Assessment and Regional Threat Supplements
- developing security policy
- managing security clearances
- investigating security incidents
- promoting security awareness
- training Security Officers

Key Security Roles: Industry Chief Security Officers (CSO)

The CSO is responsible for oversight of security arrangements, and championing a security culture in the Industry Entity.

They have flexibility to delegate the day-to-day management of protective security to their Security Officers where required.

They ensure the implementation of any recommendations from annual assurance reporting.

The CSO must be an Australian citizen able to obtain and maintain a Personnel Security Clearance at the Baseline level or above, as appropriate with the Industry Entity's level of DISP membership.

Key Security Roles: Security Officers

The frontline security professional most people are familiar with are Security Officers – if you have a security clearance, you will have a Security Officer.

Get to know yours, they provide immediate security advice to staff and to management.

Security Policy

The Defence Security Principles Framework (DSPF) is the primary security policy for Defence personnel, Contractors, Consultants and Outsourced Service Providers, to manage security risks.

The DSPF is a principles-based approach to better support Defence to manage security risk now and into the future. The DSPF is designed to enable managers to make risk-based decisions for their respective business areas.

It builds on the Australian Government Protective Security Policy Framework (PSPF) and Information Security Manual (ISM) by providing a clear governance framework including defined Defence security roles, responsibilities and accountable officers.

Security Policies and Plans outline procedures for industry entities with a goal to contextualise protective security and the DSPF for the local environment.

What is security?

Defence has five key security objectives:

1. To protect Defence's people from harm
2. To protect Defence information, assets and infrastructure from unauthorised access, sabotage, wilful damage, theft or disruption
3. To ensure that only reliable and trustworthy persons, with a need-to-know, can access sensitive or official Defence information and assets
4. To prevent unauthorised disclosure of official information, whether deliberate or accidental
5. To protect the information and assets of other nations, in accordance with security agreements and obligations between Australia and those nations

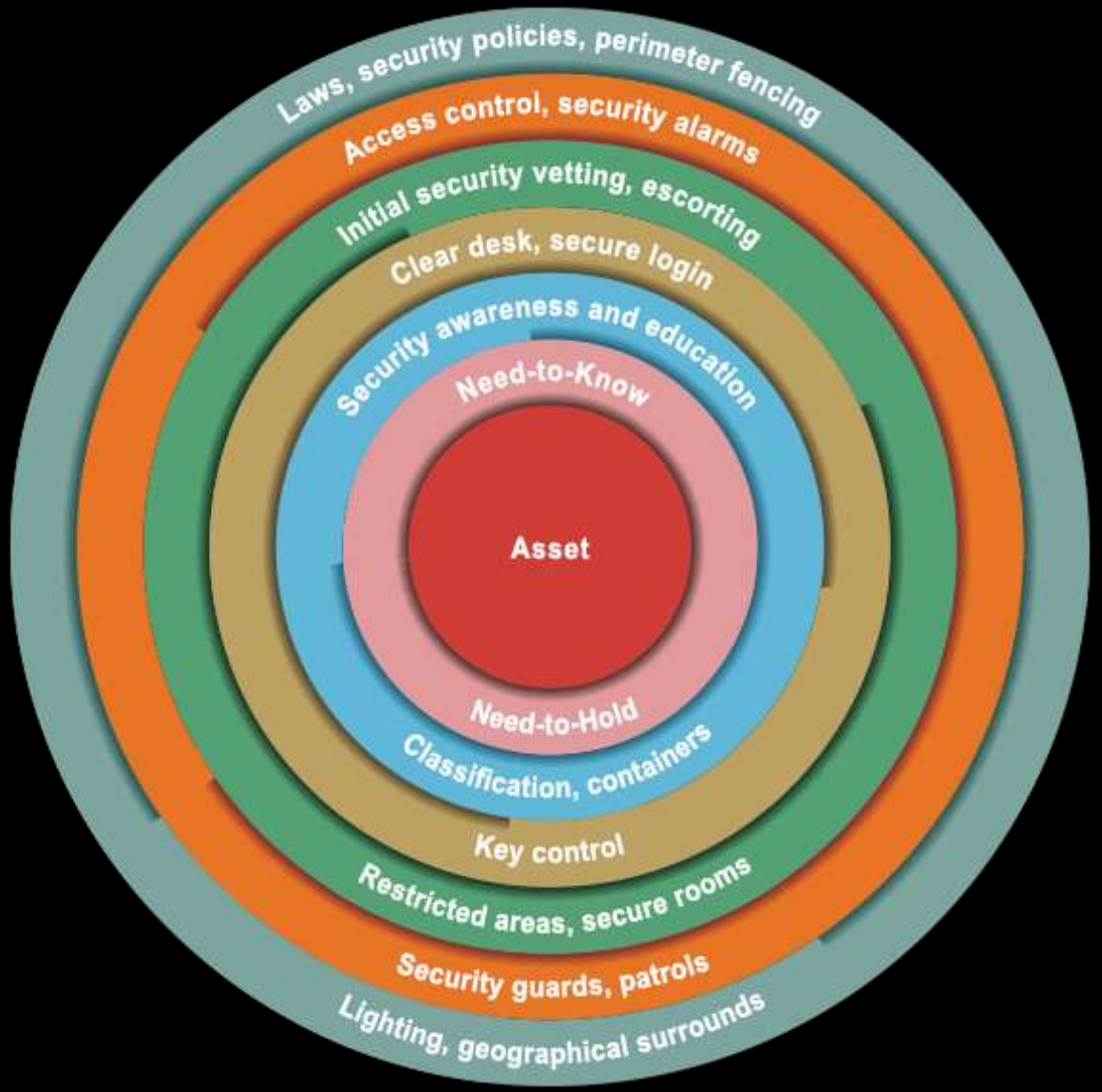
What are the threats that make security important?

- **Foreign intelligence services:** Foreign governments may try to elicit information on Australian Defence capabilities, activities or intentions.
- **Insider threat:** Involves current or former Defence employees who have, or had, legitimate access to Defence resources and have intimate knowledge of how the organisation operates. They can be a threat and/or enabler for a range of other threats.
- **Terrorism:** Individuals or groups may use violence or threats to intimidate the government and the public in order to advance their political, religious or ideological cause.
- **Criminal groups:** Individuals or groups that engage in illegal activities such as cyber attacks, illicit drug use and theft of Defence resources such as weapons or explosives.
- **Issue-motivated groups:** are a collection of activists with a common ideology who engage in political activity. Defence recognises that Australians have a legal and legitimate right to protest. Defence is only concerned about protests that are likely to be violent or disruptive.
- **Maverick individuals:** A maverick individual is an issue-motivated person, possibly a disgruntled ex-employee, who sees value in causing disruption.

Security-in-Depth

Security outcomes are best achieved through a layered approach. Defence achieves its security objectives by applying multiple layers of security measures and procedures to protect key assets. This approach is known as the Security-in-Depth principle.

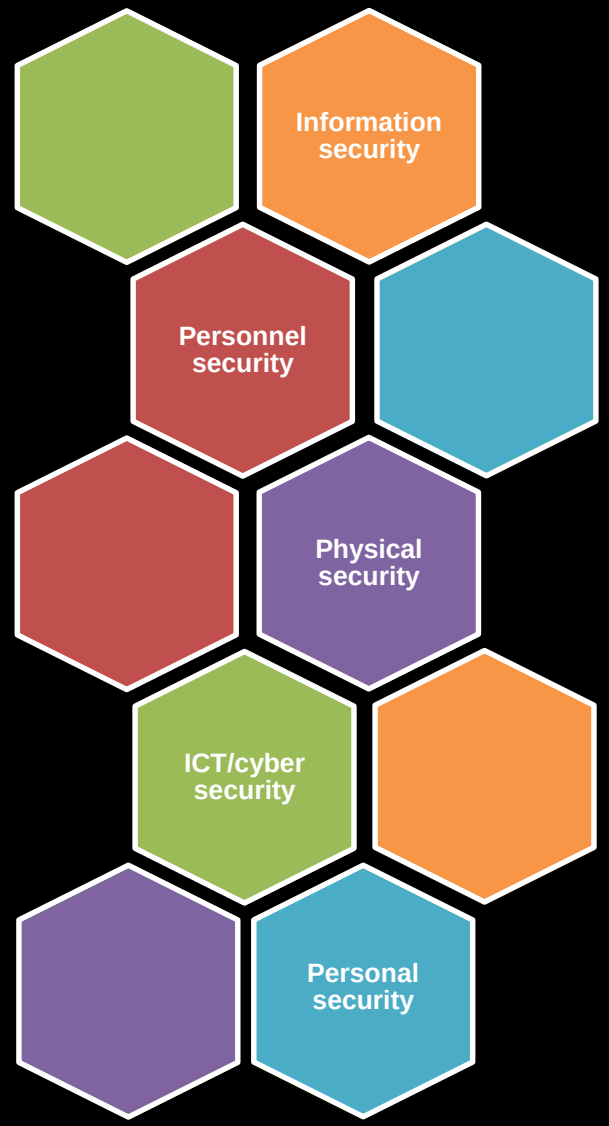
This layered approach improves security because a series of protective measures is more robust than a single line of defence. Security-in-Depth uses security protocols, processes and controls that complement and strengthen each other.



Protective Security

Protective security assists Defence and industry protect their people, information and assets, at home and overseas. So what are key considerations of protective security?

- **Information security** protects official information from unauthorised access or modification, whether in storage, transit or processing.
- **Personnel security** ensures that only people who are deemed suitable and have a genuine need to access official information and material are able to do so.
- **Physical security** provides a safe and secure environment to protect employees and visitors, prevent unauthorised access to official information and material, and to deter, detect and delay intruders.
- **ICT security** protects official information stored or transmitted in electronic formats.
- **Personal security** impacts our professional and personal lives. Your security responsibilities do not end when you leave the office. Protecting yourself and your family at home is also an important attribute of protective security.



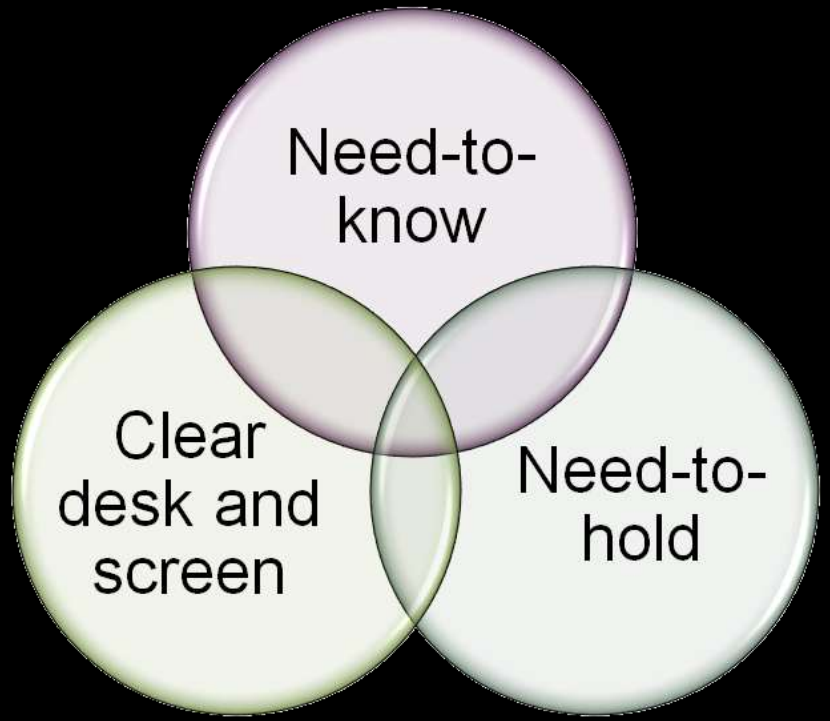
These security measures are used to protect people, assets and official information from Threat Actors.

Information Security

Information security a procedural system that protects official information from unauthorised access or modification, whether in storage, transit or processing.

Official information includes any information received, developed or collected while working for Defence, and may include:

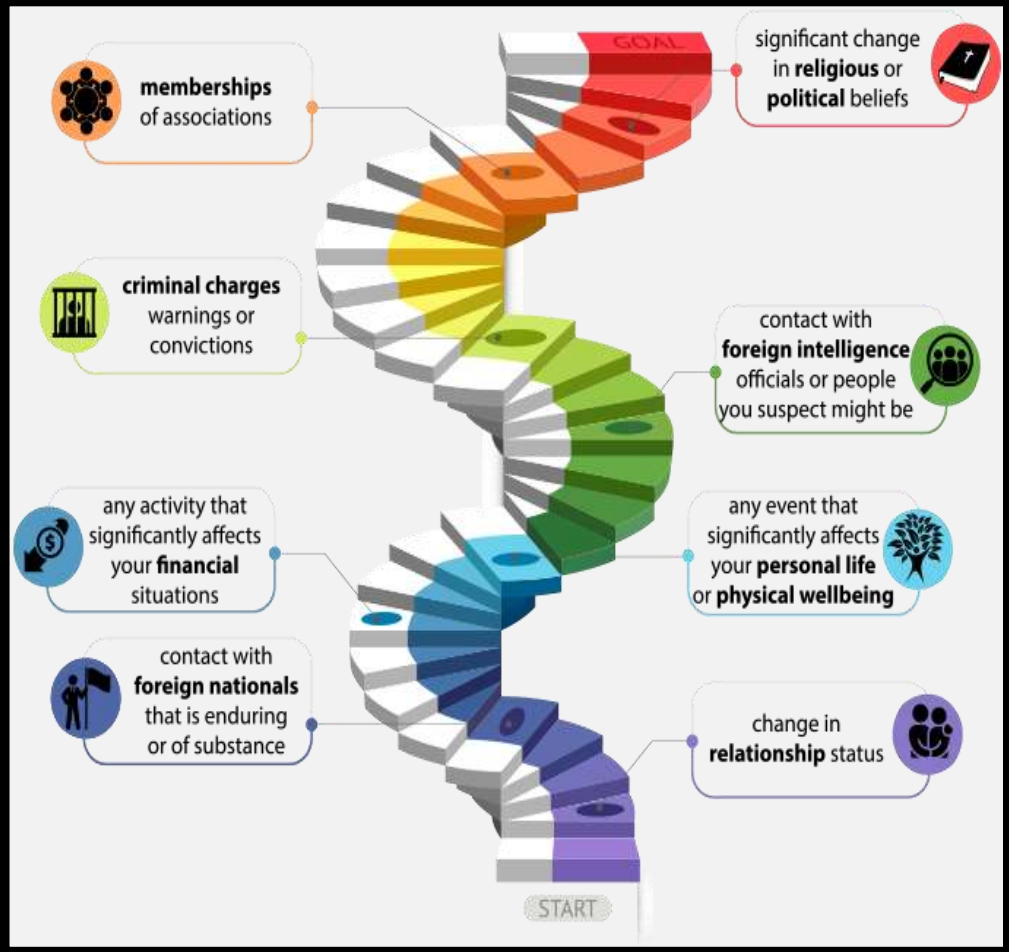
- Documents, papers and data
- Software or systems and networks on which information is stored, processed or communicated
- Intellectual information and knowledge acquired by individuals
- Physical items from which information about design, components or use could be derived



Personnel Security

Personnel Security ensures that access to official information, equipment and assets are limited to personnel who:

- have had their identity established
- are suitable to have access
- are willing to comply with the Defence and Government policies, standards, protocols and guidelines that protect Defence resources (people, information and assets) from harm



Personnel Security - vetting

The **Australian Government Security Vetting Agency (AGSVA)** is responsible for granting, revalidating and re-evaluating security clearances on behalf of non-exempt Australian government agencies and some state and territory agencies.

An applicant is assessed to determine whether they are:

- honest,
- trustworthy,
- mature,
- Tolerant, and
- loyal.

A decision is then made whether the applicant is suitable to hold a security clearance and to be granted access to classified information.

Physical Security

Physical security refers to controls such as physical barriers, access control systems, alarm systems, and security controls used to protect official information, assets and most importantly – our people. They are implemented at Defence establishments to:

- Provide a safe and secure working environment for employees and visitors
- Assist in preventing unauthorised access to official information and resources
- Deter, detect, delay and respond to intruders

Types of physical security include but are not limited to:

- Security keys
- Combination locks
- Passes
- Security zones
- Cameras
- Guards

ICT and Cyber Security

Information and communication technology (ICT) security is about protecting information stored and transmitted in electronic format. This includes security measures concerning:

- computers (including internet and social media)
- phones
- faxes
- multi-function devices; and/or
- cyber and multimedia.

ICT and Cyber Security

Spam	• **Spam** is the electronic equivalent of junk mail. The term refers to unsolicited bulk, and often unwanted, email, eg. adverts for pharmaceutical products
Phishing	• **Phishing** emails attempt to collect personal or financial information or attempt to infect your machine with malware (malicious software)
Spear phishing	• **Spear phishing** emails are highly specialised attacks against a specific target, or small groups, to collect information or gain access to systems. Eg. Crafted emails with specific Defence related themes
Whale phishing	• **Whale phishing** is a term used to describe a **phishing** attack that is specifically aimed at wealthy, powerful, or prominent individuals.

ICT and Cyber Security – Social Media

The common use of social media, no matter the medium, has increased exponentially and continues to be embraced. This has led to a blurring of lines between professional and social electronic activity which can present personnel and physical security issues.
There are consequences for personnel caught using social media inappropriately, including possible disciplinary action or criminal prosecution.

Be sure to:

- Lock down your profile to those that you want to have access
- Use strong passwords or phrases
- Be aware of what you post
- Be mindful of location and geotagging functions
- Consider how much information about you can be accessed by others

Personal and Security Culture

Strong protective security awareness and measures are important however, in order for these to be effective a strong security culture is critical.

Your positive actions help to protect information and assets.

The **‘8 Security Essentials’** provide everyone with a core set of fundamentals and accountabilities that provide a solid foundation for a strong security culture.

Reporting a security incident

As good as security measures may be, a threat actor may be able to expose a vulnerability and commit harm to your entity. Part of a good security system is knowing what to look for and when to report it.

For DISP members working on Defence projects, it is important to understand reporting obligations.

Security reporting provides valuable information on the health of the security environment and allows Defence to work with people and areas to address current and future issues.

Security Training

Annual Security Awareness course: Face to face delivery by your Security Officer or via CAMPUS. **Mandatory for all staff**.

Classified Document Handling course: For access to official information marked CONFIDENTIAL and above. via CAMPUS.

Basic Document Handling course: For access to official information marked PROTECTED and below. via CAMPUS.

Security Risk Management (SRM) workshop: For those who conduct base or security planning, capability development or project work. Delivered face to face.

Security Officer training course: Defence and DISP Security Officers to complete on appointment to Security Officer role and every three years thereafter.

Cyber Security Awareness course: Provides a basic level of knowledge of cyber security for all users of Defence ICT. Delivered through CAMPUS.

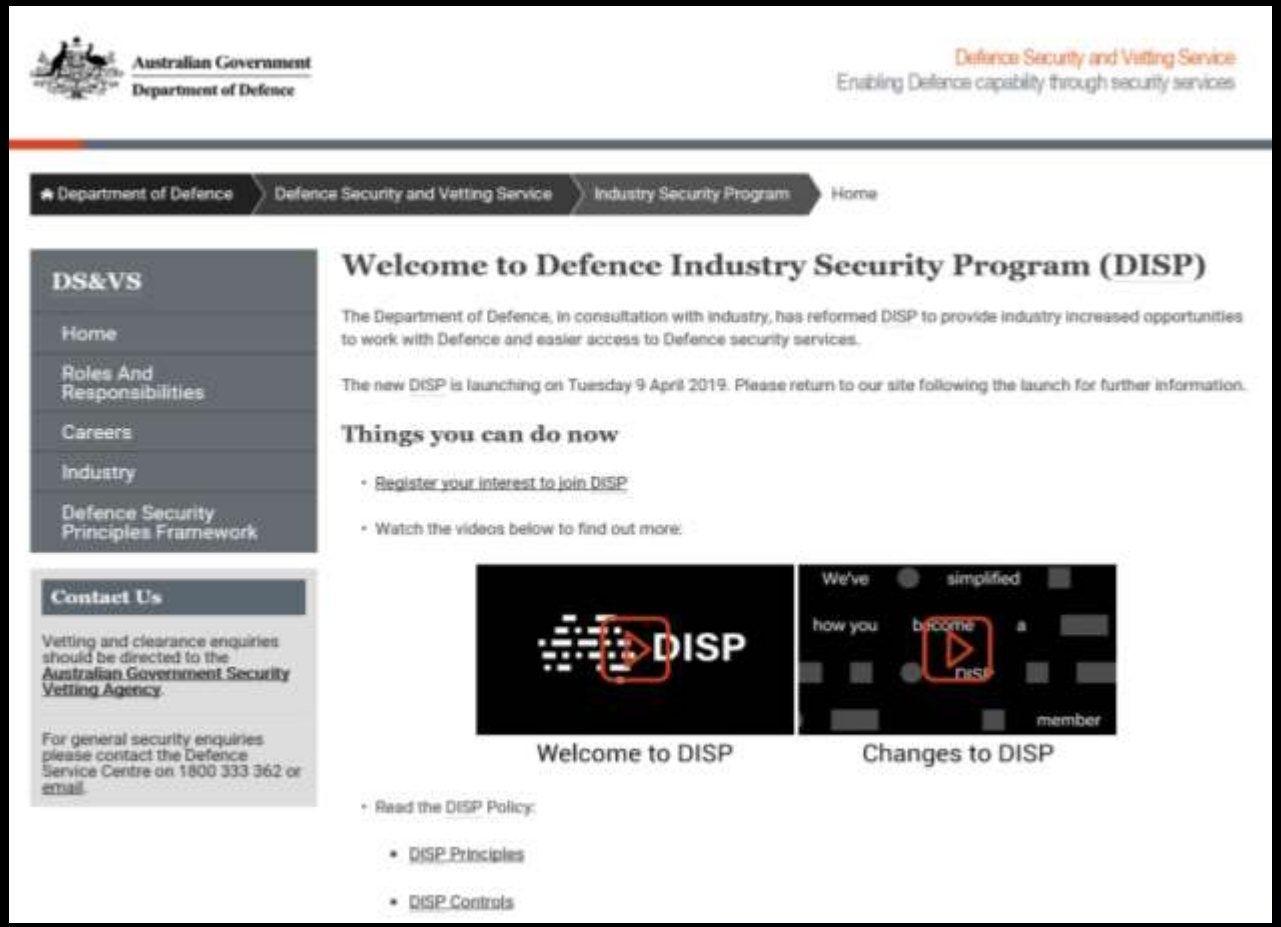
It is important, that as a member of a DISP entity, you seek further security training.

Speak to your Security Officer or your DISP Sponsor for more information.

DISP and Security Advice

Find further information on the DISP Security Internet Site:

- **http://defence.gov.au/dsvs/industry**
- Call **1800DEFENCE** (1800 333 323)
- Email yourcustomer.service@defence.gov.au



Defence Industry Security Program