



Australian Government
Department of Defence

Security Officer Resource Guide



What is the Security Officer Resource Guide?

This Resource Guide has been created by the Building Security Capability team within the Defence Security Division to support the Security Officer Course. It has been designed as a user-friendly 'plain-English' publication to provide you, the course participant with:

- basic information regarding your duties
- show you how your duties relate to the much larger security picture based on security risk management principles
- show you where to go to for advice

The Resource Guide introduces you to more authoritative sources of information such as the Defence Security Principles Framework and the Defence Industry Security Program Security Portal; it does not act as a replacement for them. As handy as this guide will be, you should **always** seek advice and key messaging from the primary sources of security information.

The Resource Guide is designed with brevity in mind. Your course facilitator will elaborate key concepts to you and show you where to find further information.

The Resource Guide will be updated on a regular basis to meet demand and changes in policy and process. By referring to the online version of this product on the DISP Security Portal, you shall always have the latest version.

If there is an error within the Resource Guide, or a broken hyperlink – please contact security.awareness@defence.gov.au

What are the coloured text boxes for?

The coloured text boxes are highlights expressing key information relating to duties, or to define key policy principles or processes.



Grey boxes contain definitions, quotes, policies and principles from authoritative sources of information.



Blue boxes contain handy hints, tips, examples and key information related to Security Officer duties.

TABLE OF CONTENTS

SECURITY OFFICER RESPONSIBILITIES	5
BACKGROUND - HOW DOES SECURITY WORK?	7
Context	8
Assets	8
Security Threats	10
Security Controls.....	11
SEEKING INFORMATION.....	13
Defence Security Principles Framework (DSPF).....	13
Security Policies and Plans	18
Seeking Advice	18
Defence Security Division	19
Australian Signals Directorate – ASD Security Branch	19
SECURITY OFFICER DUTIES	20
Security Awareness & Training	20
Awareness.....	20
Information Quick Reference Guides	21
Induction and Departure Briefings	21
8 Security Essentials.....	21
Overseas Travel Briefings.....	22
Social Media and Cyber Security Awareness Briefings	22
National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018.....	24
Security Training	24
Clearance Process.....	27
Designated Security Assessment Positions (DSAP).....	27
Eligibility Requirements	28
Security Officer Duties	28
Maintaining a Security Clearance – ‘Maintenance’	31
Periodic reviews.....	31
Change of Circumstances.....	31
Temporary Access to Classified Information and Assets	32
Controlling Access	34
Controlling access to facilities, information and assets.....	35
Access Cards	35
Key Control and Combination settings	35
Security Containers	37
Audiovisual Controls	38
Incident Response and Reporting.....	39
Security Incidents.....	39
Emergency Response	39
SAFEBASE	40
Security Incident Reporting	40
Assurance Activities	43
Security Register	43
Annual Security Report	44
Protective Security Advisory Visit	44
Census/Muster	44
Self-Certification of PSZ	45
Defence Industry Security Program (DISP)	45
PRESENTATION TIPS.....	46
Delivering Security Briefings	46

Organising a Security Briefing.....	47
Creating the presentation.....	47
Presenting.....	47
Feedback.....	48
NOTES PAGES	49

SECURITY OFFICER RESPONSIBILITIES

“Security Officers are an important part of the Defence Security Community and contribute to the protection of Defence’s people, information, assets in support of its capabilities and mission. The role of the Security Officer is critical to ensure the desired protective **security culture is promoted and maintained** across Defence.

Security Officers are required to provide **DSPF advice and support** to Control Implementers, Control Officers and their Commanders and Managers on security matters, particularly on the implementation of DSPF principles, policies, processes and controls.”

- *DSPF Governance, paragraphs 67-68*

Based on this descriptor from the DSPF – a Security Officer’s main function is to:

BE A PROMOTER:

- Of positive security culture
- Of good security practices
- Of good security risk management

BE AN ADVISER AND AN ENABLER:

- Train and advise employees on how to implement the DSPF
- Brief newcomers and old-hands in your business unit on local security practices
- Assist others to find the way forward

BE A SUPPORTER:

- Support others to make your business unit safe and secure
- Support Managers to make good risk-based decisions
- Support Managers to implement the DSPF

“Supervisors and custodians of information and assets are accountable for the appropriate implementation of DSPF principles, policies, processes and controls within their workplaces.”

-*DSPF Governance, paragraph 64*

KEY DUTIES

Managers are accountable for ensuring an adequate and functioning security regime exists in your area by:

- Promoting a strong security culture; and
- Implementing best practice security

As the Security Officer (SO), you will support this by conducting the following duties:

1. Promoting security awareness and shaping security culture in your area
2. Providing security advice
3. Coordinating/conducting security training in your area
4. Delivering security briefings (eg overseas travel, induction/departure & cyber security)
5. Coordinating and assisting clearance subjects through a clearance process, including 'aftercare' activities
6. Verifying clearances for access purposes (physical, ICT, classified meetings, visitors etc)
7. Ensuring effective access control procedures to your area, information and assets are in place and followed
8. Ensuring effective key and combination control systems are in place in your area
9. Ensuring effective **audiovisual** controls are in place in your areas
10. Ensuring staff are aware of emergency/incident procedures in your area
11. Reporting/coordinating security incident and contact reports for your area
12. Assisting/conducting inquiries post-security incident or assisting a Defence Investigative Authority (DIA) during an investigation in your area
13. **As part of your area's assurance regime:**
 - a. drafting and maintaining **Security Policies and Plans** (SPPs) for your area
 - b. maintaining a **Security Register** (SR)
 - c. conducting an **Annual Security Report** (ASR)
 - d. conducting or coordinating information/asset **census/musters**
 - e. if required – conducting self-certification of Zone 2 areas
 - f. Defence Industry Security Program (DISP) members – assisting in the maintenance of DISP membership.

It is important that you discuss and plan your duties with your Manager upon commencement of the role and record key events and duties in a calendar or plan. You will need to review these regularly as circumstances may change in your area.

You support your Manager – they may assign additional duties and make the final determination on the specifics of your role. Be flexible.

Some tools, templates and guides which you will use can be found in the Security Officer Toolkit on the DISP Security Portal.

If you are required to verify, request or cease a security clearance as part of your duties, you will require access to the myClearance Portal.

Note: It is recommended that you meet with your manager/Defence sponsor (as a new SO and then annually or as required) to discuss and agree on your duties as SO in your section/area. At the back of this Resource Guide, there is a template to record your agreed responsibilities.

BACKGROUND - HOW DOES SECURITY WORK?

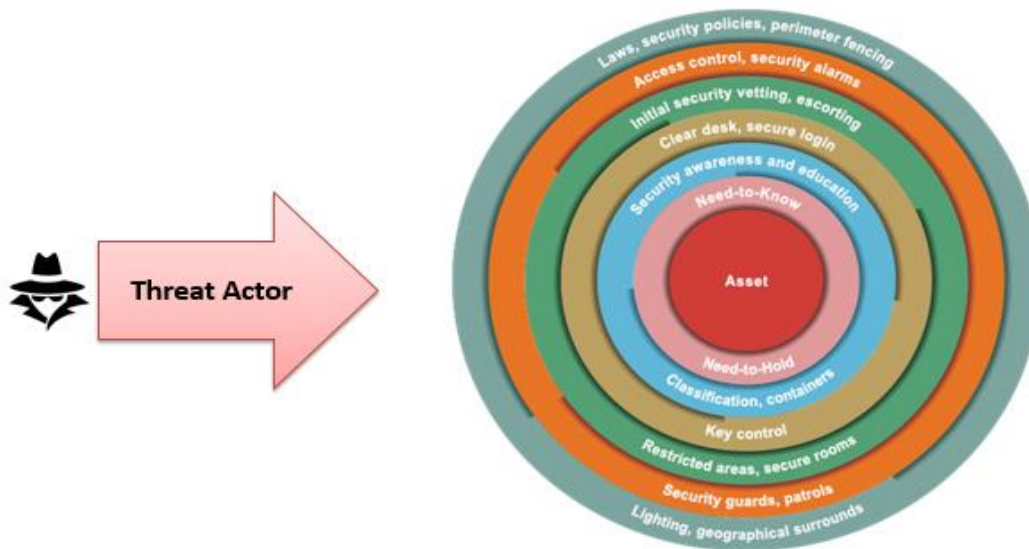
“Security is the condition of being protected against danger or loss. It is achieved through the mitigation of adverse consequences associated with the intentional or unwarranted actions of others...”

It refers to the measures used to protect assets that collectively create, enable and sustain (Defence) capability.”

- ‘Security Risk Management Body of Knowledge’

Julian Talbot and Miles Jakeman, 2008

You will remember from the Annual Security Awareness Course that protective security concerns the protection of Defence assets from threat actors using various security controls. Controls are applied using the ‘security-in-depth principle’:



Defence achieves its security objectives by applying multiple layers of security measures and procedures. This approach is known as the ‘*security-in-depth*’ principle. Security-in-depth uses security protocols, processes and controls that compliment and strengthen each other. This layered approach improves Defence’s security because a series of protective measures is more robust than a single line of defence.

What happens if security controls fail?

If security controls are not applied correctly, a vulnerability may be exposed. Threat actors like to target vulnerabilities in order to bypass security controls. In risk terms – the process of the threat actor defeating controls and attacking an asset is known as a Security Risk Event (SRE).

The realisation of a SRE is known as a ‘security incident’. Put simply ‘An occurrence which results, or may result, in negative consequences for the security of Defence’. If a security incident does occur, we need to adequately respond to it, report it, and recover from it.

Context

In reality, the application of controls is not quite as simple as the security-in-depth picture above. Security controls cannot be applied equally and effectively at an enterprise level. One area is not the same as another, even if they possess similar assets. Security must be applied taking into account local needs and unique business requirements – as per the intent of the DSPF. It is all about operational and strategic context.

Operational Context – Refers to gaining an understanding of your area’s internal environment. (What does your organisation do? What assets are you trying to protect? Why do they need protection? What makes them attractive to threat actors? What controls are already in place?).

Strategic Context – Refers to gaining an understanding of the external environment in which your area is operating or may be operating in the future (geography, social environment, legislative concerns, neighbouring factors). It also requires an understanding of any threat actors who may be interested in harming or compromising your assets.

Establishing context is the first step and most fundamental input into any Security Risk Assessment (SRA).

But what has this got to do with Security Officers?

Your Managers, those you support in making security decisions, will require information inputs into their SRAs. You can assist them. Many of the questions required to establish context can be sourced from the documents you maintain and the duties you undertake, such as:

- Security/Asset Registers
- Security Policies and Plans
- Incident Reporting
- Annual Security Reports
- Security Briefings
- Threat Briefings

As a SO, you will play a significant role in the security risk management process. You’ll learn more about SREs, SRAs and context if and when you attend the [Security Risk Management Workshop \(SRMW\)](#).

Assets



‘Assets’ is a collective term that describes items that are valued or relied on to sustain capabilities, such as people, property, equipment, information and reputation.

What makes your assets attractive?

Threat actors would not be interested in your assets if they weren't attractive to their needs. It is like a *moth to a flame* – what is it about your asset/s that makes someone want to harm, compromise, destroy or steal it?

- Is it worth stealing because of its monetary value?
- Is it worth sabotaging to make a negative impact on your capability?
- Will it benefit a foreign, industrial / criminal entity if they had access to, or information about it?
- Will it make a statement if people were harmed?
- Will it inflict damage to your business' reputation?

Knowing the answers to these questions may give an indication to the types of threats who may wish to inflict harm.

What is your asset worth to Defence?

This is not just a question about monetary value, but how *critical* is that asset to Defence capability and the national interest. What would be the *impact to business* if that asset were lost, compromised, made inoperable or tampered with? What would be the impact to Defence's reputation? Two *criticality ratings* we give information and assets are:

- Business Impact Levels (BILs), and
- Security Classifications.

The BILs/classifications help to drive the level of required security controls used to protect the information/assets.

It is a good idea to maintain an assets register. The register will indicate the type and numbers of assets and how critical they are to Defence's capability.

Is there any general advice I can give with regards to protecting our assets?

Reduce holdings to only what is required. Remember the '*Need-to-Hold*' principle – *Only have in your possession what you require to achieve the task*. Resources that have not been used or referred to for a long time should be *disposed of* in accordance with DSPF Control [DSPF Control 10.1 Assessing and Protecting Official Information - Annex H](#). The less there is to protect:

- The LOWER the security risk
- The LOWER the security overheads
- The FEWER amounts of information/assets to muster at census time!



STOP printing stuff out! - PROMOTE this concept as much as possible. Encourage the use of ICT measures to store, handle and transfer information. It is a much more efficient way of protecting information.

Security Threats



You will remember from your prerequisite training (Security Awareness Course), that there are six major threat 'actors' that Defence is concerned about:

Espionage & Hostile Foreign Intelligence Services: Other governments may try to elicit information on Australian Defence capabilities, activities or intentions. This information can be used to improve their own military capability or to harm the Australian Defence Force.

Insider Threats: The insider threat involves current or former employees who have, or had, legitimate access to information and 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 & Politically Motivated Violence: Individuals or groups may use violence, or the threat of violence, against personnel and property to intimidate the government and the public in order to advance their political, religious or ideological cause.

Serious & Organised Crime: The organisation is at risk from a wide variety of criminal activities. For example Outlaw Motorcycle Club members may target general or specific items for theft; these items may include computer equipment, weapons or explosives.

Maverick & Fixated Individuals: A maverick individual is an issue-motivated person, possibly a disgruntled ex-employee, who sees value in causing disruption. Maverick individuals are generally non-conformists, driven by a particular concern or dispute. They can sometimes be unstable to deal with, act on impulse and may make poor decisions.

Issue-Motivated Groups and Violent Protests: Issue-motivated groups are a collection of activists with a common ideology who engage in political activity. A small minority of individuals have historically employed violent, obstructive, destructive and/or confrontational tactics during protests. These actions have the ability to interfere or inhibit the organisation in carrying out its functions.

Each threat actor is unique in who they are, what capabilities they possess and what intent they have to harm or compromise your assets:

INTENT x CAPABILITY = THREAT

INTENT – the *confidence* to carry out the stated or postured claim as well as the *desire* to carry out the action or activities.

CAPABILITY – The *capacity* or *ability* of a threat actor to implement an attack.

-Security Risk Management Body of Knowledge

A national-level threat assessment therefore may not be effective for your local needs. It is imperative that you find the right threat product to assist you. Speak to your DS Division Regional Office for further assistance.

Security Controls

Physical, personnel and ICT/information security controls come in all shapes and sizes. Knowing what is necessary for your area can only be determined by:

- achieving the security principles as identified by Control Owners in the DSPF
- applying the minimum mandatory security standards as described by Control Owners in the DSPF; and
- conducting a Security Risk Assessment.

This will give you the most effective security system for your needs. But what does an effective security system look like?

We generally describe a security system using the well-known concepts of physical, personnel and ICT/information security.

Physical Security Principle: Defence facilities, people, official information, and security protected assets are protected from unauthorised access, sabotage, wilful damage, theft or disruption through a safe and secure physical environment.

Personnel Security Principle: Only those people recognised as eligible, suitable and trusted will obtain and retain access to Australian Government resources (people, information and assets).

Information/ICT Security Principle: Defence will protect official information in accordance with the expectations of the originator of the information. Where Defence is the originator of information, it will classify that information, according to the impact of access by, or disclosure to, unauthorised individuals, groups or organisations.

-DSPF Principles 72, 40, 10

Unfortunately, security is not so easily siloed into those categories. You will notice that many of the duties that you will undertake as a SO will span some if not all of these categories.

Example - Controlling access to visitors incorporates both physical (escort duties, visitor passes) and personnel (verifying security clearance) security controls.

Sometimes it is better to look at security from an emergency/security risk management point of view – P2R2 or D3R2, as described in both the *Security Risk Management Body of Knowledge* and the Handbook 167:2006 *Security Risk Management*.

It does not matter which method you use – they complement each other and fundamentally describe the same thing – **how do we apply controls to reduce/eliminate the likelihood and consequence of a Security Risk Event.**

How does it all fit together?

Let's look at a simple example based on a SRE: *'A trusted insider removes official information which is disseminated (intentionally or inadvertently) to a third party through non-ICT channels.'*

To reduce/eliminate the likelihood of this event we will try to:

Prevent (or Deter, Detect & Delay) it by:

- promoting an active and accountable security culture – 8 Security Essentials
- tightening access control measures
- reduce ability to print materials
- use Objective to store and transfer information
- remove ability to use Portable Electronic Devices (PEDs)
- conduct random security checks of the area
- conduct close-of-business checks
- conducting security awareness training
- compartment information, and
- improving morale in the area thereby reducing likelihood of malicious insider activity etc.

Prepare our staff to respond to it by:

- making them aware of their responsibilities in SPPs
- briefing them on the '8 Security Essentials'
- ensuring adequate security training takes place, and
- encouraging security incident reporting.

Hopefully adequate preventative and preparatory controls will prove too much of a 'deterrence' for the insider. The controls are designed to reduce the insider's confidence and capabilities and therefore reduce their 'intent' to attack.

If the SRE is realised and the security incident has occurred, we will:

Respond to the incident by:

- conducting a document muster
- fact finding
- changing the combinations on our security containers
- reporting the incident to the Security Incident and Coordination Centre, and
- reporting a change of circumstances via myClearance Portal.

Recover from the incident by:

- conducting and implementing controls recommended by an inquiry/investigation,
- reviewing Security Policies and Plans and Standing Operating Procedures, and
- conduct further security training

You, the Security Officer may have a role to play in all of the controls/tasks described above. You are an essential cog in every security system and every duty that you undertake plays an important part in *preventing* a security incident.

SEEKING INFORMATION

As a Security Officer, it is important that you know where to find information to support your Managers and provide advice.

The most important source of information to you is the DISP Security Portal. It contains many useful products, including:

- tools and templates,
- fact sheets, forms and guides,
- promotional materials,
- training products,
- processes,
- links to other security sites, and
- the Defence Security Principles Framework (DSPF).

If you are a DISP member you can request access to the DISP Security Portal, email disp.info@defence.gov.au or, contact your DISP processing officer.

Another important source of information for you is the [DISP website](#). It contains products that you will use on a frequent basis such as SPPs and incident reporting forms on its [Resource](#) page.



Defence Security Principles Framework (DSPF)

What is the DSPF?

The DSPF is a principles-based framework intended to support a progressive protective security culture that understands and manages risk, leading to robust security outcomes. This approach:

- *Allows* all parts of Defence to manage security within their operational context and constraints. This recognises the best security decisions are made in accordance with agreed principles, with a desired outcome in mind.
- *Ensures* the most appropriate people are setting security requirements. Those who know their business are best placed to set security standards and requirements for that aspect of Defence business.
- *Sets* clear processes and accountabilities, which underpin assurance of Defence protective security arrangements.

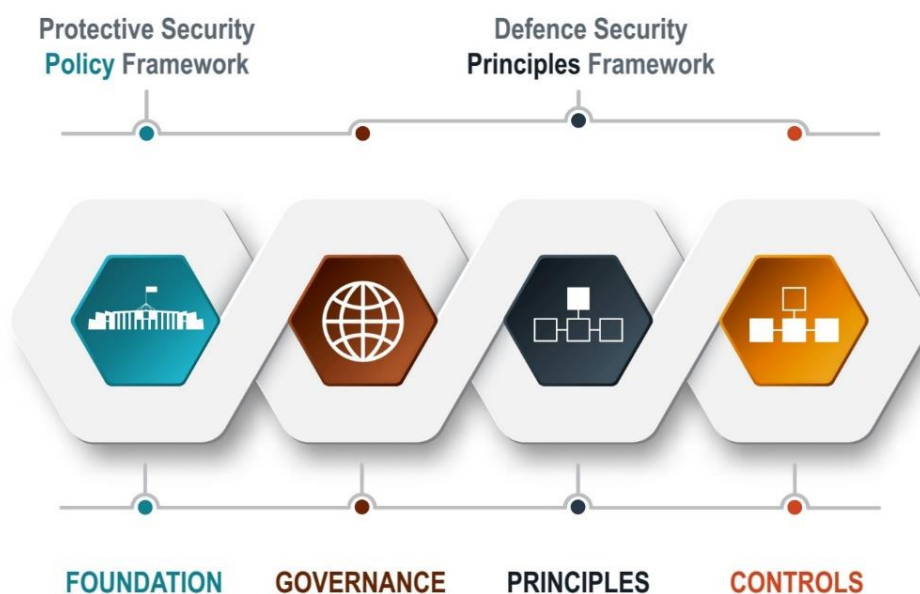
-DSPF Governance, paragraph 4

The DSPF is the primary security policy for Defence personnel, and defence industry to manage security risks. It is designed to better support Defence in managing security risk now and into the future.

The DSPF 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.

What does the DSPF look like?

There are three DSPF layers – Governance, Principles and Controls:



Governance: This layer explains the principles-based model and defines the ‘*who*’ - the roles and responsibilities, and the accountability structure for Defence. The DSPF Governance document defines the reporting and escalation structures for risks to be considered, and establishes clear roles and responsibilities for security policy in Defence.

Principles: This layer defines the ‘*what*’ and the ‘*why*’. The DSPF Principles document defines the guiding security principles that are applicable across Defence. They explain the rationale behind each principle, and outline the outcomes expected by applying these security measures. Each principle provides a statement of intent and explains the security outcomes that must be met in three parts:

- General Principle – the high-level statement of intent (this is what we need to do),
- Rationale – a statement explaining the importance of the principle (this is why we do it), and
- Expected Outcomes – a statement of what needs to be achieved in order to meet the intent of the principle (this is Defence’s desired end state).

Controls: This layer defines the ‘*how*’, ‘*when*’ and ‘*where*’. The DSPF Controls document defines further detailed controls, processes and instructions that are needed for specific security matters.

DSPF Controls provide greater flexibility and agility that cannot be delivered by applying one control unchanged across Defence. This part of the DSPF allows the Control Owner – the subject matter expert and accountable authority in Defence – to manage specific security risks more effectively, rather than being bound by a ‘one-size-fits all’ approach. DSPF Controls are authorised and released by Control Owners to meet their specific circumstances and requirements.

Who are the key players when it comes to managing security risk?

The DSPF Governance document describes the roles and responsibilities of the key positions who manage and are accountable for security risk. Such positions include:

- Secretary of Defence (Risk Owner)
- Associate Secretary (Defence Security Risk Steward)
- First Assistant Secretary DS Security (Chief Security Officer), and
- Chief Technology Officer, Chief Information Officer Group (CIOG), Chief Information Security Officer
- Your Contract Manager

As a SO, you will have minimal (if any) engagement with these positions. Read [DSPF Governance](#) for more information on their responsibilities.

Who are the key players I may engage with as a SO?

Control Owners: An SES of ADF Star Rank Officer assigned *accountability and authority* to manage a specific defence security risk as derived from each DSPF Principle document.

Control Implementers: Group Heads and Service Chiefs, or Managers of specific business units, may be specifically delegated responsibility by the Control Owners to ensure the *implementation and/or reporting* against specific controls to mitigate or manage security risks.

Executive Security Advisers: support their senior management and Control Owners to analyse their security and counter unacceptable risk; act as their Group or Service point of contact for security matters; and, provide support in maintaining an effective Security Officer structure.

Control Officers: encompass all staff and stakeholders in the Defence Enterprise. Defence personnel, contractors, consultants and outsourced service providers all have a duty to manage security risk in accordance with the DSPF.¹

Supervisors and custodians of information and assets are accountable for the appropriate implementation of DSPF principles, policies, processes and controls within their work places.

Where Defence personnel outsource a function, they cannot outsource the risk. Managers remain accountable (via the Contract Manager) for the protective security of their function and any official information and sensitive equipment made available to Contractors, Consultants and Outsourced Service Providers.

-DSPF Governance – paragraphs 56, 60, 63-66

1. As a SO, you may be a Control Officer in your area – speak to your Manager for further guidance on your Control Officer responsibilities.

How is the DSPF used to manage security risks?

If you have DPN access you are encouraged to watch the DSPF promotional/educational videos on the DISP Security Portal. They explain in detail how to apply the DSPF using risk management principles (see videos – ‘*How to work with the DSPF*’ and ‘*How to Manage Risk Locally*’ for an example of how to apply the DSPF).

As discussed in the videos, the framework allows security risks to be managed at the local level – using local solutions to meet the intent of the general principles and expected outcomes of the DSPF. Where additional guidance is required, Managers can find further advice in the DSPF Control documents.

Note: Unfortunately the videos are currently only available on the DPN.

This flexible approach to managing risks, allows Managers to make informed security decisions based on:

- Security intelligence and evolving threats
- Understanding of the local operating environment, and
- Knowledge of the unique business requirements of their areas.

Where there is a risk in achieving the expected outcomes of the DSPF, Managers are to manage or escalate the risk in accordance with sound risk management practices. You’ll learn more about these practices if and when you attend the [Security Risk Management Workshop](#).

Escalating Risk: Security risks are to be resolved at the lowest possible level. Where serious residual risks cannot be resolved, they are to be reported to an appropriate decision maker, in accordance with the DSPF. ‘Escalation thresholds’, established by Control Owners, determine the level (rank or position title) at which Defence personnel can manage risks at varying risk ratings.

Contractors, Consultants and Outsourced Service Providers *cannot manage or escalate risks except through Defence personnel.*

-DSPF Governance – paragraph 35

Escalation thresholds can be found in each DSPF Principle and Controls document.

Risk Rating	Responsibility
Low	Defence personnel in consultation with their Supervisor, Commander or Manager
Moderate	EL2/O-6 or equivalent in relevant Group/Service
Significant	AS SPS
High	Defence Security Committee (DSC) – through AS SPS
Extreme	DSC – through AS SPS

Example of escalation thresholds from DSPF Control – Overseas Travel

Mandatory Provisions: Some provisions in the DSPF are mandatory. These are identified through the use of the word **must** and **must not** (bold type). Any non-compliance is a reportable security incident. If in exceptional circumstances a mandatory provision cannot be met, a dispensation must be sought and approved by the relevant Control Owner.

Are there further resources available that can provide DSPF guidance?

DS Division has a very useful Policy Overview Page on the DISP Security Portal. Useful resources:

1. The DSPF
2. Whole of Government security policies – the PSPF and ISM
3. The Defence Security Manual (for transitional requirements)
4. DSPF Terminology Guide
5. And more....

Security Policies and Plans

You need to create and maintain a set of Security Policies and Plans (SPPs). SPPs describe how an area at the local level achieve the principles of the DSPF and other 'higher level' security publications (such as Security Management Plans).

Staff should only have to read SPPs for their local security needs; they should not have to read the DSPF or any other document to find out how security works in your area. SPPs template can be found in the [Forms and Templates page](#) on the DISP Internet site if you wish to use it (not mandatory).

Are your SPPs up-to-date?

If 'higher level' documents/publications change then your SPPs may have to as well.

Do you have a Close-of-Business Check SOP?

Good idea to create one for your area. Focus on locking up, clear desk, clear printers/photocopiers etc, close security containers/rooms, logging off etc.

Seeking Advice

Seek general security advice:

- Contact 1800 DEFENCE (1800 333 362), or email
- yourcustomer.service@defence.gov.au
- disp.info@defence.gov.au

Seek personnel security clearance advice:

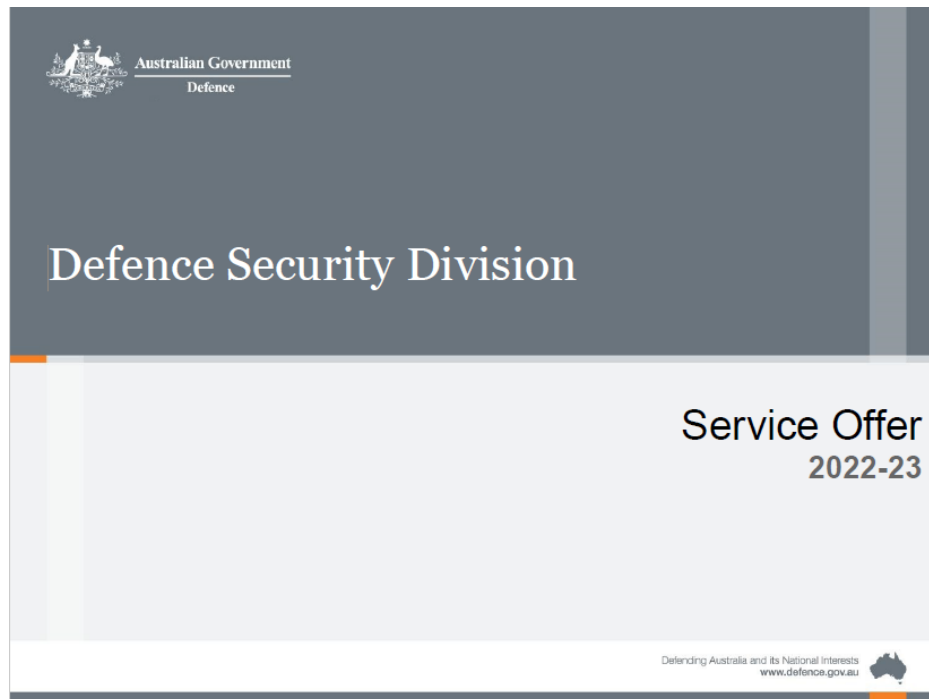
- [Australian Government Security Vetting Agency \(AGSVA\)](#)
- Contact: 1800 640 450; International contact: +61 8 8287 9192, or email
- securityclearance@defence.gov.au

Defence Security Division

DS Division – *Enabling Defence capability through security services*

DS Division enables Defence capability by providing adaptable security services that help Defence's decision makers to understand and respond to their security risks. It is important to reflect that security is a shared responsibility – we all need to play our part in reinforcing effective security culture and practices across Defence as the security environment continues to evolve.

-Defence Security Portal



Note: If you would like a copy of the Service Offer, email YourCustomer.Service@defence.gov.au.

Australian Signals Directorate – ASD Security Branch

ASD Security Branch provides comprehensive guidance on the following topics:

- Certification of TOP SECRET clearances and compartment briefings for personnel undertaking official travel or overseas deployment
- Positive Vetting (PV) clearance sponsorship
- Compartment Briefings
- Communications Intelligence Security Officer (COMSO)
- Incident response for intelligence-related product
- Defence Intelligence Agency staff reporting responsibilities; and
- Sensitive Compartmented Information Facility (SCIF) accreditation.

Contact 1800 DEFENCE if you need further information regarding the above topics.

SECURITY OFFICER DUTIES

Security Awareness & Training

Security awareness training is an important element of any protective security regime. It supports the implementation of good policies, practices and procedures and helps to foster positive security attitudes.

-DSPF Governance, paragraph 46

A strong security culture, supported by a high level of security awareness and training, is a critical element of effective security. In training staff to correctly apply security controls and follow procedures - we:

- assist in *preventing* a security incident
- *prepare* staff to *respond* to a security incident, and
- assist in *recovery* measures post security incident.

Awareness

A Security Officer promotes a positive security culture and provides DSPF security advice. What is the best way I can do that?

You will be required to advise superiors, peers and subordinates; you may brief one-on-one, small groups or on masse. You need to understand your audience. Learn how they like to receive knowledge and contextualise your product for their needs. There are some presentation tips at the back of this Resource Guide to assist you.

DS Division has a repository of security [Fact Sheets, Guides and other Awareness Products](#). We are always looking to create and improve our products, so keep an eye out for any new ones. Products include security tools/guides/pamphlets/posters etc. - feel free to use them as often as you can.

Security Risk Management

What is Security Risk Management?
Security risk management is the core principle underpinning Defence's approach to security. Defence operates on the assumption that security is everyone's responsibility and security risk management is everyone's business.

Security risk management typically includes two main elements:

- **Security risk assessment** – the process of identifying threats and vulnerabilities across all areas of security (governance, information, personnel and physical), and assessing the potential magnitude of consequences associated with those threats being realised.
- **Security risk treatment** – the process of identifying the actions, processes and resources required to mitigate or assess the likelihood or consequences associated with specific risks

What support is available for my business?
To assist in the management of security risks, Defence provides DSP members with a range of support mechanisms from a customer enquiry phone service **1800DEFENCE** (1800 333 562) and tailored security risk management training, through to online guidance, tools and templates, including up-to-date information on the sources of threat currently facing Defence.

When required, higher level support is also available through face-to-face engagement with Defence security experts who are local to your business, and can assist you in understanding the security risk assessment process and the factors that contribute to it.

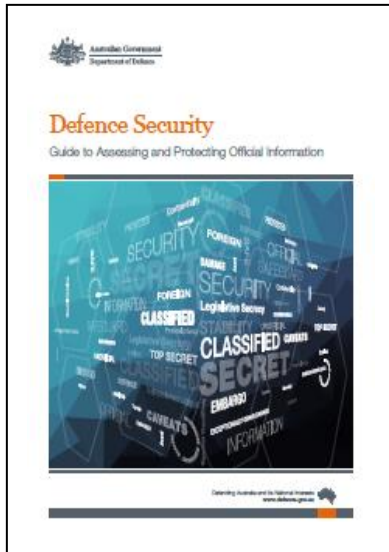
Other Policies and Information Sources

- Commonwealth Risk Management Policy
- Defence Security Principles Framework
- Protective Security Policy Framework
 - Security planning and risk management
 - Security governance for contracted goods and service providers
- AS/NZS ISO 31000:2018

Defending Australia and its National Interest
www.defence.gov.au

And more ...

Assessing and Protecting Official Information Guides



One of your peers asks you how to physically transfer SECRET documents. Your supervisor wants to know how to fill in a Classified Document Register. You could show them the DSPF. Instead, why not introduce them to the [Assessing and Protecting Official Information \(APOI\) guide](#).

Induction and Departure Briefings

You need to complete security induction briefings for all newcomers to your area. It is a duty of care as well as a means of reducing the likelihood of unintentional insider activity. Induction briefings are best conducted within the first week of their arrival. Talk to them about:

- Your local procedures – SPPs
- Your emergency procedures
- Your local controls
- The local threat picture
- Who/where to go to for security advice
- Incident Reporting
- Any other security-related controls pertinent to your area.

You need to complete a departure briefing for all staff leaving your organisation.

Note: Currently there is no set template for an induction/departure briefing – create one for your area.

8 Security Essentials

DS Division released a communications campaign for all Defence staff promoting - 8 Security Essentials in April 2021. Reviews into protecting official and classified information identified the need to communicate core personal security responsibilities and to embed a consistent Defence security culture. They address common security issues that staff at all levels may face in their roles every day, by providing simple security advice for staff to follow.

As a SO you play a vital role as an opinion leader and champion of security culture across the broader Defence community. We seek your assistance to promote the 8 Security Essentials.

DS Division have a suite of '8 Security Essentials' products that are available for order; speak to your Contract Manager who can assist you with this.

Overseas Travel Briefings

Once travel details are known by the traveller, they will complete the pre-travel sections of the AB644 *Overseas Travel Briefing and Debriefing* form and submit it to you.

As a SO, your main role is to conduct a pre-travel brief and post-travel debrief with the traveller. Let the AB644 *Overseas Travel Briefing and Debriefing* form be your guide.

Pre-travel brief: Remember to keep the discussion formal, but relaxed – you are trying to establish rapport with the traveller. This will aid with the debrief post-travel, especially if the traveller has had some security matters to relate to you.

Encourage the traveller to view and subscribe on the DFAT website: [Smartraveller](#).

Post-travel debrief: Listen carefully during the post-travel debrief – Further action may be required:

- If any security concerns are identified, forward the AB644 onto DS&VS Counterintelligence
- If any security incidents occurred – submit an [XP188 Security Incident Report](#)
- If there is a Change of Circumstance in the traveller's life – report it via the myClearance Portal.

General advice for briefing and debriefing can be found in DSPF Control 44.1 – *Overseas Travel*.

Official Travel: If a traveller is to access classified materials or gain entry to a restricted area as part of official travel, they will need to complete an *XP090 – Overseas Request for Visit or Posting Security Clearance Advice* form (see Toolkit). The form provides proof of the traveller's security clearance to the government of the country being visited. You will advise them to do this during your pre-travel brief.

Social Media and Cyber Security Awareness Briefings

The most frequent form of attack by threat actors on Government (incl Defence) and the private sector is via cyber means. It is very important that when you brief your area, you include cyber security as one of your main topics. You need to raise awareness of:

- Social media use, and
- Cyber incident reporting - SPAM and Phishing/Spear phishing.

Much of this information is contained within the Annual Security Awareness Course.

What key messages do I need to promote concerning social media?

Staff are free to use social media outside of the work environment, however, as employees of Defence or defence industry – they may be targeted through their social media accounts.

An Intelligence Collection Tool. Traditional methods of collecting information or intelligence are either being replaced by or significantly enhanced by the use of social media.

This is made much easier when:

- highly attractive information is packaged up in a single location, and

- poor security protections are in place.

Social media is frequently used by FIS, IMGs and other threat actors:

- for nefarious purposes including social engineering, phishing scams, cyberbullying and harassment;
- to gather information on organisations, its personnel, its capability and systems; and
- to identify and approach individuals of potential intelligence interest.

What information do threat actors look for on social media?

Threat actors look for vulnerabilities in an individual's online profile – information they can exploit for targeting and cultivation. Anything is useful to them, especially:

- Work profiles: What you know and what you have access to – capabilities, equipment, intelligence, technologies, etc;
- Personal profiles: Who you are – information that could be used against you such as family issues, financial problems, emotional stresses, ego, extreme views, etc; and
- 'Patterns of life': What you do & where you go – details about your routines, habits and movements.

As SOs, you need to remind your staff that when used responsibly and with the correct level of security protections applied, the risk to individuals and the organisation can be successfully managed. By remaining diligent about who can see information, as well as what information is made available can significantly increase or decrease the risk of being targeted.



Public Comment. Public comment is anything said in public or which ends up in public. If a comment has an audience, or a recipient, it's a public comment. Your company should have a policy regarding public comment – ensure staff are aware of it.

Any comment or image about Defence, or linked to Defence, could cause harm to our people, operations or reputation.

As SOs, you need to remind your staff that they need to use careful judgement before they comment on anything publicly. Once posted, it can be difficult to delete and may be replicated to people or unintended audiences.

What is SPAM, Phishing and Spear Phishing?

SPAM: Any unsolicited commercial emails (junk mail) typically of large scale to users for the purposes of advertising, phishing or spreading malware.

Phishing: The process of tricking recipients into sharing sensitive information with an unknown third party for malicious reasons. Phishing attacks are not personalised to their victims and are usually sent to masses of people at the same time, working on chance that someone will share information or inadvertently download malware.

Spear-Phishing: Is a form of targeted phishing. Attackers will target victims who disclose personal information on the internet on their profile and social networking sites. With this information, an attacker is able to act as a friend or familiar entity and send a sophisticated but fraudulent message to the victim.

- Year of Cyber Factsheet – Suspicious Emails

How do I report SPAM & Spear Phishing emails?

You need to follow your local processes.

National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018

Legislation was introduced in 2018 to deal with malicious activity involving classified information and foreign nationals - *National Security Legislation Amendment (Espionage and Foreign Interference) Act 2018*. More information regarding this can be found in the Annual Security Awareness Course.

Security Training

What do I need to do in terms of security training?

On behalf of your Managers, you may need to coordinate security training for your area. Look at your Security Register. Who needs training to fulfil a security position? Are there security vulnerabilities that could be addressed by some training?

Most people will be proactive and do it themselves, they understand the requirements of '8 Security Essentials', *apply it in your workplace*. However there will be some who need a gentle reminder of their obligations.

There may also be instances where a security inquiry/investigation recommends the need for specific training post-security incident. You are best placed to provide this training for your area.

What training courses are available?

Security training courses, both face-to-face and eLearning, are described in detail on the DISP Security Portal and the [DISP Internet page](#). Encourage staff on a regular basis to frequent the page to enhance their security knowledge and skills.

Mandatory Security Training	Who must complete	Requirement	Delivery Method
Annual Security Awareness Course	Defence personnel, Contractors, Consultants and Outsourced Service Providers.	To be completed upon commencement with Defence, and then annually thereafter.	CAMPUS Anywhere/ CAMPUS online training. ADELE LMS (code available from DISP Security Portal) SCORM packages (available from DISP Security Portal)
Assessing and Protecting official Information	Defence personnel, Contractors, Consultants and Outsourced Service Providers accessing information marked OFFICIAL and above.	All who access official information marked OFFICIAL and above as part of their duties.	CAMPUS Anywhere/ CAMPUS online training. SCORM packages (available from DISP Security Portal)
Face-to-Face Courses	Who should complete?	Requirement	Delivery Method
Security Officer	Defence personnel and defence industry employees.	For those who are about to occupy the role of Security Officer in their area.	Face-to-Face (delivered by DS Division Security Advisor).
Security Risk Management Workshop	Control Officers, Control Implementers, Commanders and Managers Security Officers are recommended to attend.	For those involved in security risk management and the implementation of DSPF principles, processes and controls.	Face-to-Face (delivered by DS Division Security Advisor).
Virtual Classroom only	Who should complete?	Requirement	Delivery Method
Security Officer course for DISP only	Defence personnel and defence industry employees.	For those who are about to occupy the role of Security Officer in their area.	Live online (delivered by DS Division Security Advisor).
ICT Security Courses	Who should complete?	Requirement	Delivery Method
Information Technology Security Officer and Manager Course	Defence personnel and defence industry employees	For those about to occupy the roles of ITSO or ITSM in their area	CAMPUS online training
Other	Who should complete?	Requirement	Delivery Method
Weapons and Explosive Ordnance Course	Defence personnel, defence industry employees and ADF Cadet unit adult supervisors	For those who handle bulk weapons and/or explosive ordnance	CAMPUS online training

Campus & Campus Anywhere. Security eLearning courses may be completed using Campus or Campus Anywhere (for those without DPN access such as Reservists, contractors, consultants and outsourced service providers). To gain access to Campus Anywhere, you must have a Campus account; which can be set up by any person with a DPN account and PMKeys ID. For further information – contact 1800 DEFENCE.

Should I attend a Security Risk Management Workshop?

Yes - especially if you are engaged in more complex security tasks (such as security risk assessments, security planning, provision of threat advice and DSPF reporting).

Security risk management is conducted for a variety of reasons across Defence, to undertake Base Planning or Resident Unit Security Plans, for capability development and project work, including with defence industry, and for building works or Certification and Accreditation of Facilities. No matter the purpose, Defence has a standardised security risk management process applicable to all Groups and Services. This Workshop aids personnel tasked with conducting security risk management by providing the latest advice and resources that will support informed judgements for the management of security risk in Defence.

The Workshop is most beneficial when conducted in location so that participants can learn with their direct stakeholders and discuss establishment-specific needs, which significantly aids in the process and end product of SRM.

-Defence Security Portal

The workshop is primarily designed for Control Officers, Control Implementers, and Commanders/Managers – those who are accountable for making security-based decisions. If they have not attended one – encourage them to do so.

Decision-makers cannot effectively manage security risk without an understanding of the basics of SRM – it is the backbone of an effective security system (as discussed earlier in this guide). More information regarding the [Security Risk Management Workshop](#) can be found on the DISP Internet page.

Clearance Process

An assured and trusted workforce of security cleared personnel is a critical protective security control. It underpins the effectiveness of many other controls and efficient business practices.

-DSPF Principle – Personnel Security Clearance paragraph 2

What are security clearances for?

The security clearance process ensures that only those people recognised as suitable, obtain and retain access to security classified information and assets.

What are the different clearance levels, and what access do they provide?

There are four levels of security clearance: Baseline, Negative Vetting Level 1 (NV1), Negative Vetting Level 2 (NV2), and Positive Vetting (PV).

It is important that staff in your area are aware that security clearances are owned by the 'position' not the 'individual'. It is the requirement of the position to access the resources below that determines the security clearance level required:

Clearance Levels	Access to Information					
	Certain Sensitive Compartmented Information	TOP SECRET	SECRET	PROTECTED	OFFICIAL: Sensitive	OFFICIAL
Positive Vetting (PV)	Y	Y	Y	Y	Y	Y
Negative Vetting Level 2 (NV2)	Y	Y	Y	Y	Y	Y
Negative Vetting Level 1 (NV1)			Y	Y	Y	Y
Baseline				Y	Y	Y

Therefore, if the position in your area only requires access to SECRET and below – there is no need for the person occupying that position to have a PV or NV2 clearance.

Even where access to security classified resources is not required, security clearances are required for individuals who work in positions of high responsibility, or may have delegations and duties that, if mishandled or abused, could cause Defence considerable harm or reputational damage (i.e. those handling bulk weapons or providing guarding services).

Register of Security Assessed Positions (RSAP)

All positions requiring a security clearance above Baseline are managed as RSAPs and recorded with the level of clearance in a RSAP. Check your RSAP (part of your [Security Register](#)) regularly with your supervisors to ensure it is accurate and reflective of what is actually required for your area. In some cases, you will need to downgrade a person's clearance if they hold a higher level than what the position requires.

Eligibility Requirements

In order to obtain a clearance, the person is required to be:

- an Australian citizen,
- have a checkable background, and
- be sponsored by an Australian Government Agency (i.e. Defence), or DISP Entity Level 1+.

In exceptional circumstances, the eligibility requirements may be waived to obtain and retain a security clearance through the provision of an eligibility waiver. It is to be noted that the provision of an eligibility waiver does not guarantee a clearance will be granted by AGSVA.

Eligibility waivers require detailed justification to be provided by the sponsor agency. This justification includes a business case linked to the capability requirement as well as a risk assessment to manage the mandatory requirements and reporting obligations.

-DSPF Control – Personnel Security Clearance, paragraph 21

Further guidance on eligibility requirements and waivers is provided in the [DSPF Control 40 – Personnel Security Clearance](#) and PSPF [Personal Security Protocol](#).

Security Officer Duties

You will assist clearance sponsors to perform their security management responsibilities including:

- Initiation of personnel security clearances (initial, upgrades and downgrades)
- Confirming clearances held with AGSVA
- Bringing to attention any clearance subjects who have not provided information to AGSVA within requested timeframes
- Revalidations
- Change of Circumstances
- Cancelling a Clearance.

AGSVA offers Security Officers guidance on the above duties on the [AGSVA website](#). In order to fulfil many of the duties though, you will need to gain access to the myClearance Portal. AGSVA also offer specific myClearance training – go the AGSVA website for further information; or access via the [GovTEAMS OFFICIAL Community](#).

To join the GovTEAMS OFFICIAL Community, you need to have a current GovTEAMS license. You can complete the [Registration Process](#) on GovTEAMS OFFICIAL, and then submit a [Log a Job Online](#) GovTEAMS license request.

On logging in to your GovTEAMS OFFICIAL account, follow these instructions to request access:

1. Select **Teams** and then at the bottom of the list, select **Join or create a team**.
2. At the top right, type **Vetting Transformation Project – SO Community**.
3. Select **Join Team**

What is the myClearance Portal and how do I get access to it?

The myClearance Portal is a 'one-stop-shop' that lets you undertake all actions from the one central place. From the myClearance Portal, you can:

- Request, confirm and cancel clearances
- Conduct clearance subject searches
- Submit changes of circumstances.

To get access to myClearance:

myClearance

OFFICIAL

Australian Government
Security Vetting Agency


Learn | Evolve | Align | Deliver

myClearance Portal User Factsheet


The **myClearance Portal** is accessed by Chief Security Officers, Security Officers, Clearance Applicants and Clearance Holders to carry out their core security clearance vetting and maintenance activities. This includes submitting clearance nomination requests, completing clearance applications and notifying AGSVA of changes in circumstances.

The myClearance Portal is accessible via a web browser on a desktop, laptop or tablet screen.


To access myClearance, you will need



A compatible smart device to download the myGovID app



To create your [Digital Identity](#) with at least a Standard identity strength



Access to the [myClearance portal link](#) on the AGSVA site

First time login

1. Download the myGovID app to your compatible device, enter your details and verify your identity to create your Digital Identity.
2. Visit the AGSVA home page to access the link to the myClearance Portal. Follow the prompts to complete the authentication process.
3. You will be redirected to myClearance to enter your personal details. This links your Digital Identity to your profile in myClearance.
4. Finally, you will be prompted to log off myClearance, before logging back in to access your profile.

Subsequent logins


1. Visit the AGSVA home page to access the link to the myClearance Portal.
2. Select Continue with Digital Identity and follow the prompts to log in with your myGovID.
3. When you receive the 4-digit code in your browser, log in to your myGovID app on your smart device to enter the code and verify your identity.
4. The myClearance Portal will match with your profile and log you in.

For more information about your Digital Identity or how the Australian Government Digital Identity System works contact: digitalidentity@dfa.gov.au

If you experience any problems with myClearance please phone 1800 640 450 or email at securityclearances@defence.gov.au

For information or support on myGovID visit: www.mygovid.gov.au

OFFICIAL


Australian Government

How do I request a new (initial) security clearance?

When an individual requires a security clearance, you will initiate the clearance process. This involves:

- Confirming clearance level requirement from the DSAP
- Go to myClearance Portal and submit a sponsorship request: Once you've confirmed the individual doesn't already have a security clearance, you will select 'Request new clearance.'
- Fill in appropriate details of the individual
- Once complete and submitted, yourself and the clearance subject will receive an email notifying the clearance subject that they can start their application.

How long do clearance subjects have to complete their questionnaire?

Clearance subjects have 20 business days from receiving their logon to complete their online questionnaire and submit supporting documentation. If the clearance subject requires more time due to extenuating circumstances, you the SO can request an extension on their behalf.

How long does it take AGSVA to process a security clearance?

Processing times for each clearance level can be found on the [AGSVA website](#).

How do I request an upgrade or downgrade to an existing security clearance?

When a clearance subject's current clearance does not match the DSAP requirements, their clearance level may need to be upgraded or downgraded. This is achieved by:

- Search for the clearance subject
- Select 'Actions' and then 'Upgrade/Downgrade interest'
- Enter all required information and select 'Submit' to complete the action

How do I register an interest in an existing clearance subject?

To register an interest in an existing clearance subject:

- Search for the clearance subject
- Select 'View' to open clearance subject's information
- Select 'Actions' and then 'Register Interest'
- Select 'Requested clearance level' followed by 'Register Interest to complete the action'

How do I remove interest in an existing security clearance?

If an individual is departing your area, and you no longer need to sponsor their clearance, then you can remove yourself. This can be done by:

- Searching for the clearance subject
- Selecting 'Actions' and then 'Withdraw interest'

Note: As their SO, you need to complete a departure brief for leaving. It is important that when a clearance subject transfers to a new area that they speak to the new SO. It is the new SO's responsibility to register an interest in them.

Maintaining a Security Clearance – ‘Maintenance’

The initial security vetting process provides a snapshot of an individual at a particular point in time. Once a security clearance has been granted there are a number of responsibilities and actions that need to be met to ensure ongoing suitability to hold a security clearance.

These measures are known as security clearance 'maintenance'.

DSPF Control 40.1 – Security Clearance Process paragraphs 89-90

Periodic reviews

Clearance holders are subject to periodic reviews to assess continuing suitability to hold a security clearance:

	Baseline Vetting	Negative Vetting Level 1	Negative Vetting Level 2	Positive Vetting
Revalidation	15 Years	10 Years	7 Years	7 Years
Security Appraisal	N/A	N/A	N/A	Annual

Once initiated, you as the SO, and the clearance holder will receive a notification email when triggered. You are required to access myClearance to confirm the clearance is still required at which point a request is issued to the clearance subject.

Change of Circumstances

Some significant personal circumstances may be used by foreign governments, issue motivated groups or criminal organisations to coerce staff into providing information or assets belonging to Defence. Commercial organisations may also use changes in circumstance to gain information that would give them an unfair advantage in dealings with Defence. When Defence and AGSVA are aware of changes to an individual's personal circumstances, it is less likely that these changes can be used as a lever and become a security risk.

Reportable changes in circumstances include but are not limited to:

- Major financial changes
- Overseas travel
- Criminal and legal matters such as court hearings or arrests
- Health issues such as mental health
- Changes to personal or contact details
- Changes in relationship such as marriage, divorce or new additions to the family
- Unusual changes in behaviour or appearance
- Long periods of absence
- Passport – Personal, Official and Diplomatic
- Significant breaches of security.



Self-Reporting. All security clearance holders are obliged to maintain high standards of integrity to keep their security clearance and to report to AGSVA any changes in their personal circumstances

for security clearance purposes. Self-reporting to AGSVA is done via myClearance Portal. As a SO, you need to remind your colleagues of their requirement to self-report.

Monitoring security attitudes and behaviours. As a SO, you and your Managers are to:

- Monitor the attitudes and behaviours of security cleared staff; and
- Encourage all individuals to report significant changes in behaviour of their colleagues where they feel it may impact on security of the area.

Where there is a noticeable change in attitude or behaviour, or any incidents that may be a security concern, you (or the Manager) are to promptly report to AGSVA using the myClearance Portal.

Simply:

- Search for the clearance subject
- Select 'Actions' and then 'Report notifiable information'
- Enter all required information and select 'Submit' to complete the action.

This becomes urgent if there is any indication that a person intends to reveal classified or other official information, or to compromise the security of Defence assets or personnel. This information is to be handled in the strictest confidence.

It is important that Managers take positive action in dealing with a potential incident like this. Do not wait for AGSVA to respond before committing to other mitigating actions (such as restricting access to information/assets, counselling, assurance activities etc).

Temporary Access to Classified Information and Assets

For urgent operational or business needs, people without the necessary security clearance may be granted limited and controlled, temporary access to classified information and assets. The approval of such access does not constitute the granting of a security clearance.

-DSPF Principle 41.1 – Temporary Access to Classified Information and Assets

Temporary access is only approved when there are no other current clearance holders available to carry out the required duties. There are two types of temporary access – 'Short Term' and 'Provisional'.

Short Term: used where access to security classified information is required by a person who does not have the appropriate security clearance. (Form SVA046).

Provisional: access can be approved after a person submits all information required for a security clearance, but before the clearance is finalised to allow that person to access security classified information on a limited basis only. (Form SVA046).

To access the forms, email securityclearances@defence.gov.au.

As a SO, you will assist Managers to process temporary access requests in accordance with [DSPF Control 40.1 – Temporary Access to Classified Information and Assets paragraphs 18-20](#). Speak with your Contract Manager first before going through the process.

Authority to approve temporary access:

Access To	Type of Temporary Access	
	Short Term	Provisional
Information requiring a PV as a prerequisite to access	Unavailable	Unavailable
Caveat / CODEWORD / Compartmented material of any classification	Unavailable	Unavailable
TOP SECRET excluding CODEWORD. ¹	Group Head, Service Chief or approved delegate in consultation with AGSVA	Minimum of SES Band 1/07 (or approved delegate) in consultation with AGSVA
SECRET and below, excluding CODEWORD	Commander, Manager or Contract Manager in consultation with AGSVA Senior Australian Defence Force Officer (SADFO) – only for SAFEBASE related emergencies	SADFO - only for SAFEBASE related emergencies

1. Clearance subjects are to hold an Australian Government security clearance at minimum of NV1 for access to this level of material under Temporary Access arrangements. (for *MOPS Act* staff, see PSPF – Australian Government Personnel Security Protocol 'Temporary Access for *MOPS Act* staff').

Controlling Access

Controlling access to facilities, assets, information and ICT systems is a *preventative* measure designed to *deter*, *detect* and *delay* threat actors. Access controls are also designed to provide safe and auditable movement for those with a need-to-know, appropriate security clearance and legitimate requirement for access.

Need-to-know principle - Defence personnel, contractors, consultants and outsourced service providers are to ensure that access to official information is limited to those who need to know the information for their official duties.

-DSPF Control 10.1 - Classification and Protection of Official Information paragraph 9

Many people associate access control with Physical Security, however the duties you will undertake as a SO clearly show that this is not the case. Access controls are equally applied using Personnel and Information/ICT controls. Your responsibilities may include:

- Verifying clearances for the provision of:
 - Unescorted access to facilities
 - Escorted access to facilities by visitors
 - Sponsoring identity/access cards
- Ensuring an effective key and combination control system is in place, and
- Ensuring effective access controls are in place to protect people, information and other assets.

What access and physical security controls are required for your area?

That depends on some basic factors as described earlier in this resource guide:

- What assets do you hold and how attractive are they?
- What are the BILs of your assets, or what are they classified?
- What is the threat activity in your area?
- What does your SRA determine?

Once you understand the answers to these questions, you will then understand the most appropriate Physical Security Zone (PSZ) required for your needs (see [DSPF Principle and Control Physical Security](#)).

ASIO Technical Notes (available in the DISP Security Portal) describe what access and physical security controls are required for each PSZ, including Security Construction and Equipment Committee (SCEC)-Approved controls and services.

What is SCEC?

The Security Construction and Equipment Committee (SCEC) is a standing interdepartmental committee for the evaluation of security equipment and services for use by Australian Government agencies. Through ASIO T4, they evaluate:

- security controls for their suitability of use in PSZs; and
- security services provided by commercial entities – such as locksmiths, couriers and security zone consultants.

Once a control or service has been evaluated and approved for use – they will be referred to as SCEC-Endorsed or SCEC-Approved.

SCEC-Endorsed controls are published in the [Security Equipment Evaluated Products List \(SEEPL\)](#).

Information regarding SCEC-Approved Service Providers can be found in the Security Toolkit on the DISP Security Portal.

Controlling access to facilities, information and assets

Access Cards

*Note to DISP SOs – You will not be involved in the sponsorship of Defence Common Access Cards (DCACs). Guidance is retained below to inform you of what is required if you or a colleague needs a DCAC from an ADF/APS sponsor.

Unescorted Access. If a staff member requires a DCAC for unescorted access to your area, you as the SO (or the DCAC Sponsor – usually the supervisor) will need to complete an AE 294 form.

It is essential though, for good security outcomes, that you identify three key things before approving unescorted access:

- They are who they say they are (proof of Identification such as driver's licence will suffice). You need to do this face-to-face.
- They have a real need for access. Check for proof – contracts, posting signals, duty statements etc.
- They have the appropriate security clearance for the area. You need to check this via the [Dashboard](#).

Escorted Access

Visitors (those without a DCAC or a legitimate reason for ongoing access to the area) may require escorting to their destination. You may need to get involved, especially if they are attending a classified/sensitive meeting. You will need to verify their security clearance (via myClearance) on behalf of the visit host. For further information regarding visitor protocols – read the DSPF Control [DSPF Control 74.1 Access Control - Annex A](#).

HINT – Advise the visit host/escorting officer of what you expect during the escorting process (ie ensure the visitor signs in the visit register; they keep an eye on the visitor at all times; they escort the visitor *straight* to the meeting room – no scenic route; etc).

Good idea for the escorting officer to brief the visitor on any security emergency and lockdown procedures for the site – this is a duty of care.

Key Control and Combination settings

Depending on the lock and keying system in your area, you may require a SCEC-Approved Locksmith to provide you a service. Get to know your local SCEC-Approved locksmith - they can be a very valuable service for your keying/locking needs.

Do you have an effective key control system in place?

- Reduce the amount of keys held – you probably only require a primary and duplicate of each key.
- Do you know the whereabouts of keys at all times? – Maintain an effective security key register.
- If you have an Electronic Key Cabinet (EKC) it may automatically have audit-trail capabilities. If this is the case – you do not need to keep a separate key register.
- EKCs may be required for higher level Physical Security Zones (PSZs) and recommended if you have a large amount of keys.
- Recommend that personnel receive a key, open or close what they need to, and return the key to you/EKC as soon as possible. Recommend that keys are NOT issued to personnel on a long-term basis. It is recommended that keys do NOT leave the facility.

Who is responsible for changing the combination settings on a lock?

Custodians need to change the combination setting at least every six months – Not You! Be aware the custodian also needs to change the combination setting if:

- There is a compromise
- A change of custodian or other person knowing the combination leaves,
- After servicing, or
- After installation of a new lock.

When was the last time the combination settings were changed in your area?

Check your [Security Register](#) for the answer.

The custodian doesn't know how to change the setting. What should I do?

Show them. There should be manufacturer's instructions that accompany and are stored within the security container. If not – you can always look it up on the internet.

Once a custodian changes the setting, and records the details in the correct manner – they will hand the details to you. Give the combination setting the same level of protection as the most valuable information/asset contained by the combination.

****DO NOT store the combination in the same container the combination opens****

Security Containers

If you print out information – you may need a security container to store it in, see the following table for guidance:

Classification	Zone One	Zone Two	Zone Three	Zone Four	Zone Five
OFFICIAL	Lockable container	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access	Secured from unauthorised access
OFFICIAL: Sensitive	Lockable container	Lockable container	Lockable container	Lockable container	Lockable container
PROTECTED	Ongoing storage not recommended, if unavoidable SCEC Class C	SCEC Class C	SCEC Class C	Lockable container	Lockable container
SECRET	Not permitted	Not permitted	SCEC Class B	SCEC Class C	SCEC Class C
TOP SECRET	Not permitted	Not permitted	Not normally permitted. (In exceptional circumstances SCEC Class A)	Not normally permitted. (In exceptional circumstances SCEC Class B)	SCEC Class B

STORAGE AND HANDLING. The [Assessing and Protecting Official Information guide](#) provides information on storage and handling requirements for each classification level.

Audiovisual Controls

Audio-visual security is measures undertaken to secure classified information from compromise by unauthorised persons through surveillance or other technical collection methods. Ensuring that classified information is communicated within appropriately security accredited facilities is the primary measure taken to mitigate audio-visual security risks. Modern, well-concealed, covert surveillance devices (bugs) are unlikely to be detected in the short term, prior to harm being caused. The first line of defence is appropriate protective security.

-DSPF Control 22.1 – Audio-visual Security paragraph 6

What are Technical Surveillance Countermeasures (TSCM)?

TSCM is the name given to a number of measures taken to identify and mitigate potential vulnerabilities and or deliberate audiovisual attack on Defence facilities. As a SO, you may need to organise TSCM services for your area, especially if you have a certified Audio Secure Room in your area. Contact 1800 DEFENCE for further information.

What is an Audio Secure Room?

A certified Audio Secure Room is a room that is rated ASL3 or above and has been certified as such. Audio-security Level (ASL) is a designation that describes the level of audio-security certification of a facility. If you want to learn more, see [DSPF Principle and Control 14: Audio-visual Security](#).

Is there any guidance regarding the hosting of sensitive meetings?

There is a Sensitive Meeting Fact Sheet and Sensitive Meeting Register/Checklist for use in the DISP Security Portal.

What is a Portable Electronic Device (PED) and what do I do with them?

PEDs are the more common term for mobility devices:

Mobility Device: A portable computing or communications device with information storage capability that can be used from a non-fixed location. Mobility devices include mobility phones, smart phones, portable electronic devices, personal digital assistants, laptops, netbooks, tablet computers, and other portable internet-connected devices.

-DSPF Control – Mobility Device Security paragraph 48

There are three categories of PEDs – Corporate, medical and personal. This is important, as restrictions on which type you carry may apply in specific areas.

Some areas within Defence are categorised as PED-Prohibited Areas. These areas are not allowed to have unauthorised PEDs carried in them due to their ability to record and transmit data. Typical PED-Prohibited areas include those that handle SECRET and TOP SECRET information, and any area deemed necessary by the Manager based on the outcomes of an SRA.

Your role, as a SO, is to ensure that PED-Prohibited Areas are clearly sign-posted, adequate containers are provided outside to store PEDs and general security awareness of the area.

Incident Response and Reporting

After a security incident has occurred, it is imperative that staff:

- effectively *respond* to the incident,
- report the incident to the appropriate security authority, and
- apply any *recovery* measures recommended by an incident inquiry/investigation.

Overall management of incident response and reporting remains the responsibility of the Managers of the area impacted. As the SO, you are to actively monitor the incident throughout the entire response/recovery process to ensure appropriate action takes place at each stage.

Security Incidents

What is a security incident?

A security incident is a suspicious approach, event, or action (whether deliberate, reckless, negligent, or accidental) that:

- fails to meet the expected outcomes of Defence security as outlined in the [Defence Security Principles Framework](#)
- compromises Defence's protective security arrangements, and
- results in (or has the potential to) loss, damage, disclosure, or harm to Defence information, assets, and people.

Examples include, but are not limited to:

- an unauthorised person accessing your facilities
- loss, theft or unauthorised access to official or classified Defence information
- loss or compromise of your access pass/security keys
- inappropriate handling or storage of official or classified Defence information or materials
- cyber security incidents
- any contacts with or approaches from people which are suspicious or unusual.

Depending on the nature of the incident (did it involve weapons, data spill, loss of an asset etc.?) further response and reporting may be required. See [DSPF Control 77 – Security Incidents and Investigations annex A](#) for further information.

Emergency Response

Note: This section applies to Defence bases and is retained below for your awareness.

All areas are to have incident and emergency response procedures in place. Resident units on a base are to have their procedures align with the base's Emergency Management Plan (EMP) & Security Management Plan (SMP). The EMP details local incident management procedures, and the SMP establishes the routine security posture on the base and details additional security controls to apply at higher SAFEBASE alert levels.

You, on behalf of your Commanders/Managers, are to ensure that all staff are aware of their responsibilities when it comes to emergency/incident procedures. This can be achieved through

SPPs and supported by an effective training and awareness program (see ‘8 Security Essentials’ No 1 & 3). It is also important that visitors to your area are aware of emergency/incident procedures – it is a duty of care. Ensure that staff who are assigned escorting duties for visitors are aware of this responsibility.



SAFEBASE

SAFEBASE is Defence’s security alert system, it communicates the threat of violent acts on Defence premises. It is a risk management and response tool underpinned by effective security planning (see your base’s SMP for more information).

There are three levels AWARE, ALERT & ACT as per the diagram on the left. As a SO, you are to ensure that staff in your area are familiar with their responsibilities and responses at each alert level:

SAFEBASE Security Alert System – Guidance for Individuals

Alert Level	What the alert levels mean to you:
Aware	<p>Understand: Defence has no knowledge of a threat to my establishment but I should be aware of my security responsibilities – and expect normal business.</p> <p>How should I behave?</p> <ul style="list-style-type: none"> • I understand security threats and risks, what they mean to me and my work area. • I am familiar with local security instructions and controls specific to my workplace - every Defence establishment is different. • I know my Unit Security Officer and where to get security help. • I report security concerns and incidents.
Alert	<p>Understand: Defence has reason to believe there is a threat, and an attack could happen at my establishment. I should take steps to enhance my personal security and the security of my area – and expect increased security measures and restricted business.</p> <p>How should I behave?</p> <ul style="list-style-type: none"> • I seek information and advice from my chain of command. • I have reviewed security instructions for my work area, focusing on actions I need to take in the event of an incident. • I take part in exercises organised by my SADFO/Base Leader. • I am mindful of additional security controls that may impact my day-to-day activities (eg. the SADFO/Base Leader may close an access point or carpark). • I am considering the potential risks to pre-planned events, exercises or meetings (eg. I consider postponing an exercise held on base or I might move a meeting to another Defence establishment). • I am keeping an eye on the establishment’s communications channels (eg. email) for new instructions or updates. • I report security concerns and incidents.
Act	<p>Understand: An attack is either imminent or happening on my establishment. I should exercise extreme caution and follow emergency procedures - and expect severely restricted business</p> <p>How should I behave?</p> <ul style="list-style-type: none"> • I am following civilian police instructions (eg. Australian Federal Police or state/territory police). • I am following emergency procedures (eg. evacuation or lockdown routines) and instructions from my wardens, security authorities, SADFO, Base Leader or Chain of Command. • I am taking care to avoid putting myself or others in harms way. • My normal work has stopped and, if it is safe to do so, I have secured classified information. • I report security concerns and incidents, but only when it is safe to do so. • If I am not inside the establishment, I will avoid the area.

Security Incident Reporting

The Security Officer undertakes the security incident reporting duties on behalf of their Commander or Manager. However, overall management of the incident and reporting process remains the responsibility of the Commander or Manager. While in the first instance security incidents should be reported to the relevant Commander or Manager, and/or the Security Officer, if the Security Officer is unavailable the individual identifying the incident is to report the incident as soon as practicable.

-DSPF Control 77.1 – Security Incidents and Investigations paragraph 12

Why is reporting a security incident important?

Defence's ability to detect, assess and mitigate security vulnerabilities depends upon accurate, timely and consistent reporting of all security incidents. The information collected and analysed in security incidents aid Defence in strengthening its defensive posture against insider threats, foreign intelligence services and other threat types.

Staff need to be made aware that if it looks suspicious – they need to REPORT IT. Ensure that staff who are exposed to an incident or a contact RECORD as much detail as possible (number plates, timings, physical features, facial descriptions, event details etc.) – this will aid you drafting the incident report. It is best that you 'over report' than 'under report' – the more details the better.

How do I report a security incident?

If you feel something is potentially life threatening or significant in nature – act immediately – EMERGENCY RESPONSE – Call '000'

For all other security incidents, including suspicious contacts, you need to submit a Security Report (found on the DISP Security Portal). If you cannot access the report, then email your account of the incident to the Defence Security Incident and Coordination Centre (SICC) – security.incidentcentre@defence.gov.au

The report/email needs to be submitted to Defence within 24 hours of discovery of the incident. Ensure you copy in your Defence Contract Manager.

What happens after the security incident is reported?

Once the security incident report is received by the SICC, they will determine which incidents are subject to further formal investigation, and which ones can remain with and be managed by the reporting Manager. If the incident is sufficiently complex or serious in consequence, the responsibility for investigating will be transferred by the SIC to a Defence Investigative Authority (DIA).

Managers are to continue managing the incident in consultation with the DIA during the investigation process.

How do we recover from a security incident?

Findings and recommendations will be produced after an investigation or local inquiry is conducted. DIAs will ensure that all recommendations from the investigation/inquiry are assigned for implementation to all areas affected by the recommendation.

Information collected through incident reporting and security investigations helps Defence identify security threats, risks and vulnerabilities, evaluate the effectiveness of security controls, develop and improve security policy, make informed and data driven security decisions, and identify security review priorities.

Timely and appropriate management of security incidents also helps Defence contain the effects of security incidents, and to recover more rapidly from adverse security events through effective consequence management.

-DSPF Principle 77 - Security Incidents and Investigations paragraphs 3-4

As the SO, you may be able to leverage off the recommendations and create training/briefing packages for your area.

Assurance Activities

What is assurance?

A process that provides confidence that planned objectives will be achieved within an acceptable degree of residual risk.

- *Security Risk Management Book of Knowledge*

By conducting assurance activities, you on behalf of your Manager, can provide *confidence* to others that:

- information and assets stored, handled and shared will be protected in a manner consistent with the DSPF; and
- the *prevention (or detect, deter, & delay), preparation, response and recovery* controls in your security system are efficient and functioning correctly.

Some assurance activities that you will conduct or coordinate include:

- maintenance of [Security Policies and Plans \(SPP\)](#)
- maintenance of a [Security Register \(SR\)](#),
- conducting an [Annual Security Report \(ASR\)](#),
- requesting and assisting with a Protective Security Advisory Visit (PSAV),
- conducting a document census/muster,
- self-certifying [PSZ Zone 2 areas](#),
- presenting security briefing/awareness sessions, and
- participation in the Defence Industry Security Program (DISP).

Security Register

A SR complements SPPs and is designed to capture all matters of security interest relevant to the area not detailed in the SPPs. It:

- represents the **present state of security** in your area
- collates all security information into one area
- provides an audit trail for assurance purposes.

Example: Local requirements for security briefings in SPPs would be supported by the registration of security briefings in the SR. As a further example, SPPs would refer to any local requirements associated with security containers, while the SR would detail the location of security containers and record combination changes.

As the SO, you will maintain a SR on behalf of your Manager. It is recommended that your Manager inspect the register no less than quarterly to maintain effective oversight of security issues affecting your area and for which they are responsible.

You can find a template for a SR in the Security Officer Toolkit on the DISP Security Portal and on the [DISP internet site – Forms and Templates](#). The template is divided into numerous worksheets covering a range of data capture topics that are recommended as part of any security register.

TOP TIPS:

- Make sure it exists, it is accurate and is up-to-date:
 - An accurate SR will assist you when compiling information for your annual AC064 - *Protective Security Self-Assessment*
 - Security Authorities will ask to see your SR during any audit/advisory visit.
- Use the SR as a guide when conducting handover/takeover with the previous SO. Go through each table and conduct the corresponding activity. Only enter your name into the register (Table A2), once you are **satisfied** with the state of it.
- Contextualise the register for your needs. If certain tables do not apply – remove them.

What other assurance activities will I conduct or coordinate?

Annual Security Report

On an annual basis, you will need to complete an [ASR](#). The ASR is a declaration by the Chief Security Officer (CSO) that your business entity is continuing to meet the DISP eligibility and suitability requirements.

Once the form is complete – your CSO needs to submit it annually to DISP.submit@defence.gov.au within ten business days of the original membership grant date.

Protective Security Advisory Visit

A PSAV is a visit to a Defence area or DISP member by DS Division for the provision of protective security assistance and advice. They are conducted as required and can address many concerns. PSAVs are not to be used for simple issues – they are mainly aimed at addressing complex issues such as:

- protective security for infrastructure changes;
- remedial action for an isolated security issue;
- implementing recommendations from a Protective Security Survey or as a result of a security investigation; or
- re-accreditation of a specific security area following refurbishment or alteration.

Simple issues can be addressed by contacting 1800DEFENCE. To request a PSAV, SOs can fill out a PSAV Request form from the DISP Security Portal.

Census/Muster

Census/Musters are conducted to ensure that assets and information that are registered to the area are accounted for. [DSPF Control 10.1 Classification and Protection of Official Information – annex F](#) has some excellent information regarding file census/document musters, including when and how they are to take place.

Check your Security Register – when is the next key, document or asset muster due?

Classified Document Register (CDR)

A CDR is used to register all SECRET, TOP SECRET and Accountable material in the area. A CDR Supervisor (essentially the custodian of the information within the CDR) is responsible for its maintenance.

Self-Certification of PSZ

If required, you may have to self-certify your own Zone 2 area. DS Division has a [Certification process](#) to help you out (contact your Regional DS Division office for more information). Certification is part of an overarching Accreditation process that provides assurance that adequate security controls are in place to protect assets and information.

Certification – is a formal assurance process resulting in a statement (certification report) that outlines the extent to which a facility conforms to controls for the required Security Zone, and as required by the DSPF

Accreditation – is the process by which an authoritative body gives formal recognition that required security standards have been satisfied and, where applicable, associated residual risks have been accepted by a facility and/or asset owner for the operation of a facility. The outcome of the accreditation process is an authority to operate for a particular facility and/or asset.

-DSPF Control 73.1 - Physical Security Certification and Accreditation

Self-certification may seem like a complex process - it is important that you contact DS Division when commencing for assistance and advice.

Defence Industry Security Program (DISP)

The DISP enhances Defence's ability to monitor and mitigate the security risks associated with contracting for, or outsourcing of – services, functions and capabilities.

The DISP is a risk mitigation and assurance program maintaining the integrity of Defence's capability by ensuring defence industry maintain security responsibilities and safeguard the supply chain. It also improves industry's ability to protect themselves from threats.

All DISP members MUST comply with the DSPF.



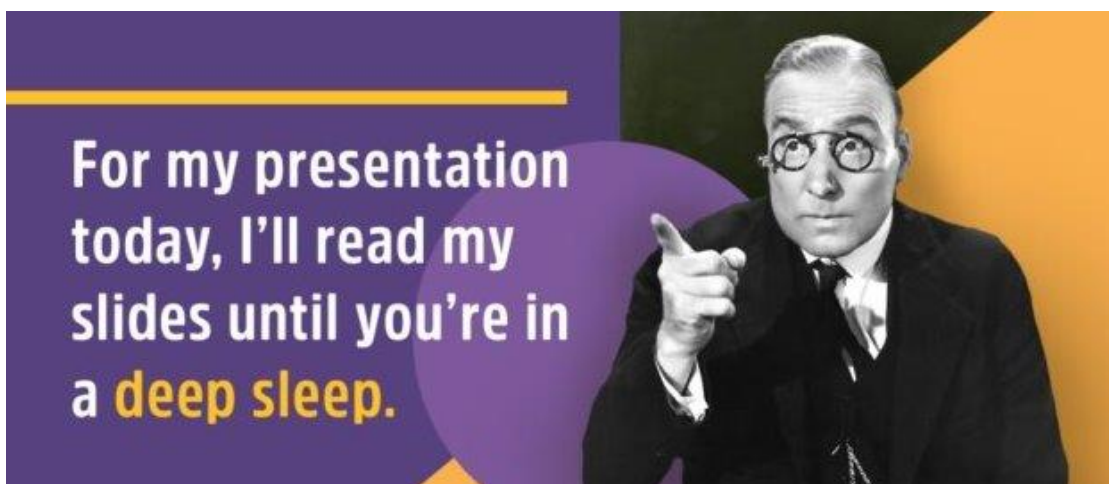
PRESENTATION TIPS

Delivering Security Briefings

There are no rights or wrongs when it comes to delivering a brief. It is entirely up to you. Every presentation is different due to the subject, the audience and the presenter. The best security training or awareness program is one that gets the point across in a variety of ways.

Deliver the product in a style that you are comfortable with. Ensure it gets your message across and that it resonates with your audience. Even a boring or serious topic can be made interesting & entertaining if you put a little effort in. An engaged audience will walk away from a presentation learning at least one new thing.

Below are some handy hints when it comes to preparing your presentation.



Briefings can be given verbally, in writing or a combination of both. If an individual's knowledge of security is poor, a combination of verbal and written briefings is recommended.

Lectures are the most common form of instruction, but lectures may not retain interest unless accompanied by training aids, a variety of topics and/or the use of guest speakers.

Discussions are best used when small groups are involved. They are ideal for unit leadership groups.

Audiovisuals are suitable training aids, shown either in full or as extracts used in conjunction with lectures or discussion.

Notices on bulletin boards serve as useful reminders, but need to be topical and changed frequently to retain impact.

Posters are useful in attracting the attention of employees to basic security measures, but again these need to be topical and changed frequently to retain impact.

Newspaper cuttings/extracts can be useful in creating security awareness when displayed for short periods of time.

Organising a Security Briefing

Before delivering a briefing, the following should be considered:

- What is the purpose of the brief?
- What security issues are you addressing?
- What information needs to be presented?
- Who is the audience?
- What is the classification of the brief?

Creating the presentation

Below are some tips to assist in creating the presentation:

- Choose the type of briefing to be given (eg. Threat brief)
- Research the topic – look at the DSPF and Security Portal – speak with DS Division or other Security Officers. Your presentation must be current and factual.
- Identify the audience – who are they, how do they like to receive information?
- Select the delivery method (eg. PowerPoint)
- How much time have you got?
- Outline the purpose of the presentation, stick to it
- Choose your embellishments: whiteboard, flip chart, videos, visual aids etc.
- If using PowerPoint slides:
 - Use correct templates
 - Standardise style
 - Include only necessary information, be disciplined
 - Be consistent with effects, animations, colours etc.
 - Make it engaging – use pictures, tables, diagrams etc. as much as possible
 - The audience is there to listen to you, not read the presentation on the screen – restrict slide content to a minimum!
- Practice
- Know your venue – what is available to you. Good idea to visit the venue well in advance of your presentation to test your equipment. Nothing worse than delaying a presentation due to technology-failure.
- Have a contingency plan.

Presenting

Be clear, accurate and engaging.

Active involvement from participants should be sought, encouraged and valued. Take your cues from the audience, observe their body language and participation – that will give you an immediate indication of your performance.

Use your voice and watch your pronunciation, emphasis, pace, pitch, projection, volume and grammar. Eliminate jargon and slang and overuse of acronyms. Keep it simple – not everyone is a security expert – use language they can identify with.

Do not be offensive. Ensure your presentation complies with equity and diversity requirements.

Find natural pauses in your presentation and ensure participants have a break.

Be as natural as you can, use gestures and expressions in a natural manner. Don't be afraid to use some humour – even in a security presentation. A well placed quip works well, but can also ruin your presentation if at the wrong place and time. If you're not a funny person, don't try it in the first place.

Sometimes it is a good idea to be 'mobile' on stage. Try not to get stuck behind a lectern – moving towards and amongst your participants is engaging.

It is okay to respond with 'I don't know'. There is nothing worse than presenting false facts or answering the question inadequately. In the break, research an answer to the question and get back to the participant as soon as possible.

Always conclude by reinforcing the purpose of your presentation.

Feedback

Where appropriate – seek feedback on your presentation. Feedback helps you to improve your performance for the future.

Your agreed key responsibilities as a Security Officer

No	Task	Date commenced	Date completed	Comments
1				
2				
3				
4				
5				
6				
7				
8				
9				
10				
11				
12				
13				
14				
15				
16				
17				
18				
	SO signature : Manager signature:			

Note: It is recommended that you communicate and consult with your Manager/Defence sponsor regularly.

