

ANNUAL SECURITY AWARENESS

eLEARNING WORD DOC VERSION | JAN 2021

**DEFENCE SECURITY & VETTING SERVICE**

© Commonwealth of Australia 2021

This work is copyright. Apart from any use as permitted under the *Copyright Act 1968*, no part may be reproduced by any process without prior written permission from the Department of Defence.

All classified Defence information is protected from unauthorised disclosure and it is an offence to release classified information under the *Criminal Code Act 1995* and the *Privacy Act 1988* .Information contained in Defence publications may only be released in accordance with the Defence Security Principles Framework.

**Publication title:** Annual Security Awareness eLearning – Word Doc Version

**Edition:** Version 1

**Sponsor:** Building Security Capability | Defence Security & Vetting Service

**Developer:** Defence People Group | Design & Development

**Effective date:** 29 January 2021 | **Review date:** 1 January 2022

**AMENDMENTS**

Proposals for amendment of the ASA Word eLearning - Word Doc Version may be sent to:

Security Professional Development | Building Security Capability

Defence Security & Vetting Service | Department of Defence

DSVS.skilling@defence.gov.au

Campbell Park Offices | Campbell | ACT 2612

|  |  |  |  |
| --- | --- | --- | --- |
| Amendment number | Amendment | Amendment type | Effective date |
|  |  |  |  |
| Nil | Nil | Nil | Nil |
| Nil | Nil | Nil | Nil |

# 

CONTENTS

[COURSE OVERVIEW 4](#_Toc62811241)

[Course objectives 4](#_Toc62811242)

[Intro Page 4](#_Toc62811243)

[Welcome 4](#_Toc62811244)

[MODULE 1 | **Security: It is your business** 4](#_Toc62811245)

[What does security mean to you? 4](#_Toc62811246)

[Charlie’s scenario 5](#_Toc62811247)

[Reflection on what security means 9](#_Toc62811248)

[M1 | Module 1 Summary & Commitments 10](#_Toc62811249)

[MODULE 2 | **Protective** **Security 101** 11](#_Toc62811250)

[M2 | Module overview 11](#_Toc62811251)

[Understanding security 11](#_Toc62811252)

[5 KEY questions you need to ask 12](#_Toc62811253)

[Let’s apply the questions to a real life example 16](#_Toc62811254)

[What informs the application of these controls? 17](#_Toc62811255)

[What is THE Defence Industry Security Program (DISP)? 18](#_Toc62811256)

[M2 | Knowledge Check 18](#_Toc62811257)

[M2 | Module Summary & Commitments 20](#_Toc62811258)

[MODULE 3 | **How to Not be a Vulnerability** 21](#_Toc62811259)

[M3 | Module overview 21](#_Toc62811260)

[Be aware of your surroundings 21](#_Toc62811261)

[What can I do in differing work environments? 23](#_Toc62811262)

[The insider and your responsibilities to report 25](#_Toc62811263)

[Cyber: Anywhere, Anytime 28](#_Toc62811264)

[Be social media savvy 31](#_Toc62811265)

[M3 | Knowledge Check 32](#_Toc62811266)

[M3 | Module Summary & Commitments 35](#_Toc62811267)

[MODULE 4 | **Responding to security incidents** 36](#_Toc62811268)

[M4 | Module overview 36](#_Toc62811269)

[identifyING a security incident 36](#_Toc62811270)

[Inform your Commander/Manager or Security Officer of the situation 37](#_Toc62811271)

[Emergency response to a violent security incident 38](#_Toc62811272)

[M4 | Knowledge Check 40](#_Toc62811273)

[M4 | Module Summary & Commitments 40](#_Toc62811274)

[MODULE 5 | **Where to go for your security needs** 41](#_Toc62811275)

[Security Officers 41](#_Toc62811276)

[The Security Portal 42](#_Toc62811277)

[Course COMPLETE 43](#_Toc62811278)

# COURSE OVERVIEW

## Course objectives

The course objectives is divided into five key modules/themes:

1. **Personal Accountability** | Module 1
2. **Protective Security 101** | Module 2
3. **How to Prevent Security Incidents** | Module 3
4. **Responding to Security Incidents** | Module 4
5. **Where to go for your security needs** | Module 5

[Return to Table of Contents](#Table_of_Contents)

# Intro Page

## Welcome

Welcome,

Annual Security Awareness (ASA) is undertaken by all Defence personnel including industry on an annual basis in order to understand individual security responsibilities.

Throughout you'll make a number of commitments designed to encourage you to make good security choices. These commitments will form part of your Completion Certificate which you can use to reflect upon your security behaviours throughout the year.

Knowledge check – there is no pass mark to complete the ASA. The questions are designed to measure the security maturity within Defence and defence industry. Answer the questions honestly. Defence Security & Vetting Service will analyse the results of the knowledge checks in order to shape better product for you.

# MODULE 1 | **Security: It is your business**

## What does security mean to you?

**What do you think of when you hear the word security?**

Typical responses to these questions are…

|  |  |  |
| --- | --- | --- |
| Security isn’t really  my business… | It won’t happen to me... | That’ll never happen… |
| Staff displaying relaxed attitudes on security awareness. | | |
| Nothing ever happens  in my area… | No one ever gets in trouble around here… | As if I’ll ever need this… |

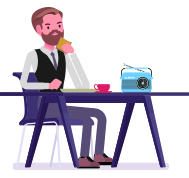
Let’s have a look at Charlie’s story in the following scenario.

[Return to Table of Contents](#Table_of_Contents)

## Charlie’s scenario

This is Charlie, a Defence employee. Let’s see Charlie’s attitude towards security in this scenario…

**Scene 1: Breakfast before work.**



It’s Monday morning and Charlie is finishing his breakfast. On the news that morning there’s a breaking story on an incident affecting Defence capability and information due to suspected cyber activity. Charlie doesn’t pay particular attention to the news, as he’s getting ready for a busy day and rushing out the door.

**Scene 2: The commute to work.**

****

Driving to work Charlie hears the breaking news story again. The story talks about website exposing classified Defence information related to millions of dollars of high tech equipment.

Still not paying much attention to the story, Charlie changes channels to listen to some music.

**Scene 3: At the office.**



When Charlie arrives at work his workmates are talking about the leak. It was apparently hacked from someone’s personal account. They’re wondering who in their right mind would send classified information from the DPN to their Gmail account?



Charlie remembers he sent classified information to his Gmail last Friday because he wanted to save time to meet project deadlines.



Charlie’s workmates explain how he’s compromised the information, risked Defence’s reputation and put the entire project at risk.



Charlie explains he was just trying to be efficient and meet the deadline.

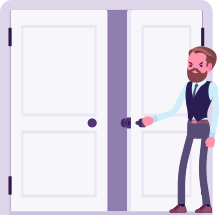


Charlie is informed that senior management have been in the boardroom all morning discussing the Security incident.



Charlie becomes greatly concerned. He thinks about how this could affect him. Will he lose his job, what this could mean for his family? He didn’t mean to cause Defence’s reputation harm.

**Scene 4: The boardroom.**



The boardroom door opens and Charlie is immediately requested to come in.

Charlie’s actions weren’t unintentional, they were deliberate.

If he listened to his Security Officer about protecting Official Information under the Espionage and Foreign Interference Act, or paid attention when completing his Annual Security Awareness he would have understood exactly what could happen to him.

## Reflection on what security means

### Reflection on typical responses to security should now be…

|  |  |  |
| --- | --- | --- |
| Security is my business… | This could happen  in our workplace… | I am accountable! |
| Staff realisation of the importance of security awareness. | | |
| This could happen to me… | I need to know more! | If I do the wrong thing,  I could be trouble… |

### SECURITY IS YOUR BUSINESS!

The *2020 Defence Strategic Update* highlights a shift in power dynamics in our immediate region and the need for greater consideration of domestic security. Security threats to Defence capabilities and activities will increase, particularly from foreign interference, espionage and malicious insiders.  Protection of critical Defence platforms and technologies is becoming more difficult.

No matter what rank or position you hold, every member of Defence and defence industry play a vital role in maintaining Defence's security. You are responsible for the protection of information and assets in your custody at all times. If you fail to protect Defence’s information and assets then you may be prosecuted under the;

* *Espionage and Foreign Interference Act 2018,*
* *Crimes Act 1914*
* *Defence Act 1903*
* *Criminal Code Act 1995* and
* *Public Service Act 1999*.

As a security clearance holder it is important to remember what you signed up for:

*I understand that all official information acquired by me in the course of my duties is the property of the Commonwealth. I will not publish or communicate any such information to another person in any form either during or after my service in or association with the Commonwealth, unless disclosure is for official purposes.*

*I further understand that any breach of laws regarding the safeguarding of official information is an offence, and may render me liable to criminal prosecution.*

*-* (Security Clearance Informed Consent and Official Secrecy Acknowledgement)

**You are accountable for your Security actions.**

As you will learn in this course, we all need to play our part in protecting what matters most to Defence. If we don’t do the right thing it could have an adverse impact on Defence business, our national security and potentially harm individuals.

**Don’t be like Charlie!**

[Return to Table of Contents](#Table_of_Contents)

## M1 | Module 1 Summary & Commitments

### MODULE SUMMARY

Below is a summary of what you learnt in this module:

1. **Security is your business**

### M1 | YOUR COMMITMENTS:

Throughout this course you’ll make a number of commitments designed to encourage you to make good Security choices. These commitments will form part of your Completion Certificate.

You are required to tick the commitments and sign (below) in each module.

**I am accountable for my Security actions.**



### MODULE COMPLETE

**Well done, you have completed Module 1 | Security: it is your business.**

The next module in this course is **Module 2 | Protective Security 101.**

[Return to Table of Contents](#Table_of_Contents)

# MODULE 2 | **Protective** **Security 101**

## M2 | Module overview

In this module we speak about the vulnerabilities and how they enable threats to harm Defence.

Module objectives:

1. Recognise the importance of these 5 key questions, and how they play a role in good Security.
2. Understand the importance of the Defence Security Principles Framework (DSPF) and your local security processes.

[Return to Table of Contents](#Table_of_Contents)

## Understanding security

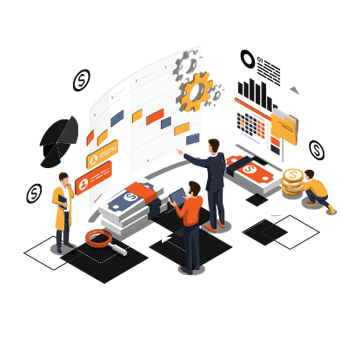
To understand security there are 5 key questions you need to ask yourself:

1. **What are we trying to protect?**
2. **Who are we trying to protect from?**
3. **What will the impact be if harm is caused?**
4. **What allows harm to be caused to these assets?**
5. **What do I/you need to do to best protect our asset/s?**

[Return to Table of Contents](#Table_of_Contents)

## 5 KEY questions you need to ask

### 1. What are we trying to protect?

****

**Assets.**

Assets is the collective term used to describe Defence’s people, information, equipment and reputation. Assets are used by Defence and defence industry on a daily basis to support our capabilities and implement Defence’s Strategic Objectives as outlined in the [*2016 White Paper*](https://www.defence.gov.au/whitepaper/) and the [*2020 Strategic Update*](https://www1.defence.gov.au/strategy-policy/strategic-update-2020).

### 2. Who are we trying to protect from?

****

**Threats.**

Due to who we are, what we stand for and what we own, Defence is an attractive target for those who wish to cause us harm. These are known as threat actors. There are six primary security threats (threat actors) to Defence as outlined in the Defence Security Threat Assessment (DSTA):

1. **Espionage & Foreign Intelligence Services (FIS)**
2. **Insider threats**
3. **Terrorism and politically motivated violence**
4. **Serious and organised crime**
5. **Maverick individuals**
6. **Issue-motivated groups and violent protest**

Each threat has a different intent and capability in how they inflict harm on Defence and our assets. Not all threat actors are considered equal. To understand what threats pose a risk to you, read the DSTA, Regional Supplements and/or talk to your local Security Officer (SO).

Let’s look at each threat actor in turn:

1. ***Espionage and Foreign Intelligence Services (FIS)*** – State based individuals whose purpose it is to ascertain information on Defences capabilities, activities and intentions. The information is used to improve their own capabilities or degrade Defence’s. FIS use different techniques to illicit information - one of which could be to exploit YOU.

It’s not only FIS who engage in espionage activities. Corporate or Commercial espionage is just as rife in the defence industry sector where the consequences both to the company and Defence itself could be catastrophic.

1. ***Insider threats*** *–* The insider threat is either a current or former employee with intimate and legitimate knowledge of how Defence operates. Insiders have access to our facilities, IT systems, information and assets. Because of their legitimate access, insiders can be used by other threat actors as a conduit to bypass Defences security controls*. Don’t be the conduit!*   
     
   You will learn more about insiders later in the course*.*
2. ***Terrorism and politically motivated violence*** *–* Individuals or groups who use violence or the threat of violence against Defence personnel and property to intimidate the Government and the public in order to advance their agenda.
3. ***Serious and organised crime*** *-* Individuals or groups who target Defence through illegal means to benefit from Defence (for example: drugs, fraud, theft and physical violence etc.).
4. ***Maverick and fixated individuals*** *–* Individuals who have a real or perceived grievance with Defence. Some may be fixated on a particular issue or individual and may act on impulse and make poor decisions.
5. ***Issue-motivated groups*** *–* Groups of activists with a common ideology who engage in protest activity. This becomes an issue when it turns violent or results in a direct action against Defence personnel, assets etc.

### 3. What will the impact be if harm is caused?



Impact to Defence and individuals will differ depending on the importance of an asset. Consequences can generally be determined by categorisations that we give to our assets such as Classifications and Business Impact Levels (BILs). Generally speaking, the higher the classification or BIL, the greater the impact to Defence.

**Impact/consequences to Defence:**

* Compromise, loss, and sabotage of assets could severely disrupt Defence’s capability and could cost Defence significant amounts in time and money to recover. Defence could lose the capability edge over our adversaries, and in severe cases – this could lead to mission failure.
* Other impacts to Defence and defence industry can be reputational where confidence by trusted partners and the public is weakened.
* The loss or compromise of a dangerous asset such as weapons, or explosive ordinance could cause physical or deadly harm to individuals.

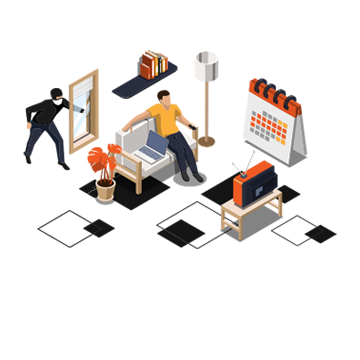
**Impact/consequences to individuals:**

If you were the cause of the harm through unintentional or malicious activity, the consequences to you could be quite significant. You may be subject to performance management, administrative action, and in some cases disciplinary action.

For example, if you were to deliberately disclose official information to an unauthorised source (just like Charlie in Module 1) – then you would have breached Defence policy and Commonwealth legislation. Under the *Espionage and Foreign Interference Act 2018* (EFI Act), such an action could lead you to two years imprisonment.

For more information on the EFI Act see the National Security Legislation Amendment Act 2018 – Espionage and Foreign Interference [(Summary of Offences)](javascript:var%20newWnd=ObjLayerActionGoToNewWindow('https://ext.defence.gov.au/sites/default/files/media/EFI-2018-Summary-of-Offences.pdf','Trivantis_','width=1025,height=701,scrollbars=1,resizable=1,menubar=1,toolbar=1,location=1,status=1');).

### 4. What allows harm to be caused to our assets?

****

**Vulnerabilities.**

Defence’s security CONTROLS are good, but only if applied correctly.

Some controls may not be as efficient and effective, most likely due to human induced error/negligence. These errors cause HOLES in the security system that a threat actor may exploit. We call these holes VULNERABILITIES.

If you don’t do the right thing or are subject to coercion, **YOU become the vulnerability**. The realisation of a vulnerability is a Security Incident.

### 5. What do we need to do to best protect our asset/s?



**We apply a layered approach using a multitude of security controls** - this is known as *‘Security-in-Depth’.*

The strength and nature of controls differ depending on the type, importance and attractiveness of the asset and the potential capabilities of the threat.

Controls can include:

* Physical security (Security doors, zones, barriers & containers)
* ICT/Information security (Firewalls & passphrase protection)
* Personnel security (Clearances & good security culture)
* Administrative/Governance (Policies and procedures)
* Training and Education

These controls are designed to prevent (**deter, detect, delay**) the threat actor from gaining access to the asset.

The more important the asset is to Defence, the more layered the security controls should be.

Part of protecting our asset is responding to and reporting of a Security Incident when it occurs. Timely response reduces the consequences of harm to the asset.

[Return to Table of Contents](#Table_of_Contents)

## Let’s apply the questions to a real life example

### 

Figure Royal Australian Navy - Submarine and ship side by side

### 1. What are we trying to protect?

One example is **Defence’s naval capability**.

From the *2020 Defence Strategic Update* we know the three strategic objective are to:

1. Shape Australia’s strategic environment
2. Deter actions against Australia’s interests
3. Respond with credible military force when required.

One way to support these objectives is with a strong Naval capability.

To modernise our naval capability Defence is spending up to $183 billion on new and improved:

* Surface and above water combat
* Undersea combat and surveillance
* Maritime warfare patrol and geospatial
* Maritime combat support and amphibious warfare.

### 2. Who are we trying to protect from?

This large shipbuilding project may be of interest to Foreign Intelligence Services (FIS).

### 3. WHAT WILL THE IMPACT BE IF HARM IS CAUSED?

* Lost capability edge due to compromise
* Harm to people
* Improved enemy capability
* Billions of dollars lost
* Reputational loss
* Technology compromise
* Loss of confidence with defence industry and coalition partners
* Loss of contracts

### 4. What allows harm to be caused to our assets?

* Insider activity, including contractors and business associates
* Cyber incidents i.e. malicious cyber attacks
* Poor information handling practices
* Poor social/audio visual awareness
* Poor Social Media discipline
* Compromise of supply chain
* Undetected surveillance
* Compromised devices
* Data Spills

### 5. What do we need to do to best protect our asset/s?

* Security training and awareness
* Cyber vigilance
* Password protection
* Strong access control measures
* Use of accredited systems
* Security clearances

**Note:** This is a very simplistic view of the 5 questions in action. The real application of the 5 questions to explain the security of naval capability is very complex and cannot be easily explained in detail.

[Return to Table of Contents](#Table_of_Contents)

## What informs the application of these controls?

**The Defence Security Principles Framework (DSPF).**

The DSPF is a principles-based document developed to support Defence in managing its security risks now and into the future. The DSPF is Defence's way of achieving whole-of-government security requirements mandated within the:

* [Protective Security Policy Framework](https://www.protectivesecurity.gov.au) (PSPF)
* [Information Security Manual](https://www.cyber.gov.au/sites/default/files/2021-01/Australian%20Government%20Information%20Security%20Manual%20(January%202021).pdf) (ISM) and,
* Commonwealth Legislation

The DSPF allows commanders and managers to develop security controls based on local needs, unique business requirements and security risk. Once Commanders and Managers have assessed what is required, they will inform those under their supervision via local security procedures. You may know these in Defence as **Security Standing Orders (SSOs)** and for defence industry **Security Policies and Plans (SPPs)**. It is imperative that you understand your local procedures, by reading them on an annual basis. Speak to your Security Officer for more information.

### BEWARE – Normalised Deviance!

Normalised Deviance is the process in which deviance (unofficial alternative) from appropriate behaviour becomes normalised in a corporate culture. For example, the use of unapproved systems to communicate official information. It is usually done to circumvent a process which may be deemed obstructive or prolonged. Normalised deviance is unacceptable. Security exists for a reason. Taking short cuts or using unapproved methods creates vulnerabilities exposing Defence to significant harm.

[Return to Table of Contents](#Table_of_Contents)

## What is THE Defence Industry Security Program (DISP)?

DISP is a risk mitigation and assurance program designed to maintain the integrity of Defence’s capability and safeguard the supply chain. The program ensures defence industry meets the security standards of the DSPF. It also enhances Defence’s ability to monitor and mitigate security risks associated with contracting or outsourcing services, functions and capabilities.

DISP is mandatory for industry working on:

* Classified information or assets
* Storing or transporting Defence weapons or explosive ordnance
* Providing security services for Defence bases and facilities
* As a result of a Defence business requirement that is specified in a contract

…and encouraged for:

* businesses that supply goods and services to Defence, or work on sensitive information or assets.

Anyone working with defence industry or considering research collaboration should ensure they have a good understanding of the program. To learn more about [DISP](https://www1.defence.gov.au/security/industry), see their website.

[Return to Table of Contents](#Table_of_Contents)

## M2 | Knowledge Check

Question 1

**To understand security, what are the 5 key questions you need to ask?**

Select the correct answers.

* What are we trying to protect?
* Who are we trying to protect from?
* What will the impact be if harm is caused?
* What allows harm to be caused to our assets?
* Where do we keep our personal assets?
* When do we declare change of circumstances?
* What do we need to do to best protect our asset/s?

Question 2

**Below are six primary security threats (threat actors) to Defence. Who or why are they threats?**

Match the correct *Threat Actors* (numbers) to the *Who or Why* (alphabet letters).

|  |  |  |
| --- | --- | --- |
| Security Threats Actors | Match the pairs  (e.g. 1 = A) | Who or Why? |
| 1. Espionage & hostile Foreign Intelligence Services (FIS) | 1 = A | 1. Ascertain information on Defence’s capabilities, activities and intentions. |
| 1. Insider threats | 2 = B | 1. Can cause accidental or intentional harm to Defence due to their intimate knowledge of our controls. They could also be subject to coercion. |
| 1. Terrorism and politically motivated violence | 3 = C | 1. Use violence to intimidate Government and the public to advance their agenda. |
| 1. Serious and organised crime | 4 = D | 1. Target Defence through illegal means for financial gain or benefit. |
| 1. Maverick and fixated individuals | 5 = F | 1. Groups of people conducting protest activity against Defence. |
| 1. Issue-motivated groups and violent protest | 6 = E | 1. Individuals who aim to be destructive or disruptive to Defence, driven by a real or perceived grievance. |

Question 3

Have you read your local processes (Security Standing Orders or Security Policies and Plans) in the last 12 months?

* Yes
* No
* No, they do not exist in my unit/area
* No, I do not know if they exist or where to find them.

Knowledge Check COMPLETE

Well done, you have completed the Knowledge Check for Module 2.

[Return to Table of Contents](#Table_of_Contents)

## M2 | Module Summary & Commitments

### MODULE SUMMARY

Below is a summary of what you learnt in this module:

1. To understand security, there are **5 key questions** you need to ask:
   1. What are we trying to protect?
   2. Who are we trying to protect from?
   3. What will the impact be if harm is caused?
   4. What allows harm to be caused to our assets?
   5. What do we need to do to best protect our asset/s?
2. The DSPF supports Defence in managing its security risks now and into the future.
3. Be aware of the **Defence Industry Security Program** (DISP).

### M2 | YOUR COMMITMENTS:

Throughout this course you’ll make a number of commitments designed to encourage you to make good Security choices. These commitments will form part of your Completion Certificate.

You are required to tick the commitments and sign (below) in each module.

|  |  |
| --- | --- |
|  | I will commit to reading my local security processes on an annual basis and abiding by the regulations within. |



### MODULE COMPLETE

**Well done, you have completed Module 2 | Protective Security 101.**

The next module in this course is **Module 3 | How to Not be a Vulnerability.**

[Return to Table of Contents](#Table_of_Contents)

# MODULE 3 | **How to Not be a Vulnerability**

## M3 | Module overview

This module covers the importance of cyber security, your responsibilities and how to prevent security incidents in differing environments.

All case studies are true stories, names have been altered to protect the individuals.

Module objectives:

1. Being aware when working across differing work environments
2. Your responsibilities as a security clearance holder
3. The importance of cyber security and being social media smart

[Return to Table of Contents](#Table_of_Contents)

## Be aware of your surroundings

### scenario - Working from home

|  |  |  |
| --- | --- | --- |
| 1. C:\Users\Developer\AppData\Local\Microsoft\Windows\INetCache\Content.Word\M3_ScenarioTradie_1.jpgThis morning you are working from home and are expecting a tradesperson to arrive shortly. Just after you log into DREAMS the doorbell rings | 1. You lock your screen and answer the door to let them in. C:\Users\Developer\AppData\Local\Microsoft\Windows\INetCache\Content.Word\M3_ScenarioTradie_2.jpg | 1. While you are working the tradesperson asks you some questions about where you work, what you have been working on and if you have had any involvement with the Unified Communications roll out. C:\Users\Developer\AppData\Local\Microsoft\Windows\INetCache\Content.Word\M3_ScenarioTradie_3.jpg |
| 1. You politely answer without giving much away but confirming that you have involvement with the project. | 1. You are paying the tradesperson by the hour so end the conversation and encourage them to get back to work. |  |

### Questions to ask

* Do you take for granted the efficiency of security controls at work when you handle and discuss Official information?
* Does everyone around you have a need to know?
* Have you thought about the vulnerabilities at your home when you have that online meeting?
* Are you aware of prying eyes in the airport lounge when you decide to work on your project?
* Are you aware of how you appear to a threat actor when you are out in public?

### Protecting Official Information

You need to be aware of your surroundings at all times, especially when in uncontrolled spaces and when handling and discussing **Official information**. This includes, but is not limited to, when working onsite, from home, in-transit during travel, on operation, in the warehouse, or even in private time. You never know who or what could be taking an interest in who you are and what you do.

Any work done or received by on behalf of Government is OFFICIAL information (i.e. work related). Any information not work related is UNOFFICIAL. Further guidance can be found in the **Assessing and Protecting Official Information (APOI)** course and supporting Guide. If you have not already completed the APOI course it is highly recommended that you do so.

The APOI course should be completed on a regular basis to ensure you are aware of your information handling requirements. The [APOI Guide](https://www1.defence.gov.au/security/training-awareness/assessing-and-protecting-official-information) supports this course and is an excellent tool for everyday use.

### Be aware of what you look like to a threat actor.

Have you thought about what you might look like to a threat actor in person?

Imagine that you are at the supermarket, or at the airport, or waiting for a taxi, can you pick out a Defence employee?

* What gives it away?
* Is it the way they look or dress?
* Is it the way they talk amongst themselves?
* Is it what they have in their possession?

There are some things that you cannot change. You are who you are. However, there are some simple things you can do to make yourself less attractive to a threat actor:

* Removing lanyards, ID cards and badges when in public
* Refrain from wearing uniform while in public
* Where possible, refrain from discussing work in an uncontrolled space. Especially places of mass gathering such as supermarkets, sportsgrounds and restaurants/bars.
* Refrain from carrying hard copy materials with you in transit, between worksites, etc. Wait until you are back in a secure environment before you access Official information.

Remember in Module 2 we discussed that threat actors are attracted to assets. You are an asset and, despite what some people might say, you are attractive as well. You need to make yourself less attractive!

### What are we looking out for?

As a Defence or defence industry employee you may be at risk of a suspicious contact due to your knowledge of Defence information. Targeting can happen in both official and private settings, either in person or online.

The best way to recognise a potential approach of concern is through the acronym ‘**SOUP**’:

* **Suspicious** occurrences – Does the contact ask personal or professional questions that appear that they may already know something about you and what you do?
* **Ongoing** contact – Does the contact try to establish and maintain a relationship?
* **Unusual** incidents – Did the contact appear deliberate as opposed to a random occurrence?
* **Persistent** approaches or questioning – Does the contact continue to push for further information?

**Case Study:**

A Defence member, who works for Defence Science and Technology Group, also occasionally lectures at his local university.

At the end of one of his lectures, a supposed student approached him to discuss some of his previous work. The conversation did not seem suspicious, as he had previously lectured on such topics. The student changed the conversation to ask about current work the member is doing. The Defence member had just commenced working on a project to do with submarine propulsion. The student seemed quite interested in the project and stated that she hoped to eventually move into that area. She asked if the member had any papers that she could read.

The Defence member was excited by the enthusiasm and promised to send one of his recent papers. The Defence member sent through an OFFICIAL research paper written on Defence capability.  After sending the paper through, the Defence member did not hear from the student again.

A couple of months later, the Defence member was sent a link by his colleague to a published article in an online foreign journal. On review, the Defence member realised that it was his research paper that had been published. The Defence member reported the situation to his boss who advised him to report a security incident.  The Defence member's actions could have put the capability at risk leading to loss of edge over our adversaries or the need to abandon the research.

**Inform and report!** If you believe you have been targeted, inform your Commander/Manager or Security Officer – this is a Security Incident.

You may need to report this via a Security Report. The Security Report can be found on the Security Reporting Hub or through your Security Officer. More information is provided in the next module on security reporting.

[Return to Table of Contents](#Table_of_Contents)

## What can I do in differing work environments?

With our work environments now being more flexible it is important to understand that they can differ in the level of security provided and what we need to be mindful of when working. Let’s take a look at just some of the considerations for the various environments.

### Working Onsite

Defence or defence industry sites are the most secure as they have been certified and accredited as meeting security standards. These controls make up Physical Security Zones which are designed to allow you to work in a safe and secure environment. Do you know which zone you work in? If not, or if you would like to know more, talk to your Security Officer.

To find out what you can do at the local level, consult your SSOs/SPPs.

Things to look for include;

* Have awareness of your immediate surrounds. Does everyone have a need-to-know?
* Be mindful of the Portable Electronic Device (PEDs) policy in your area.
* Understand what level of classified speech can be conducted in your area.
* Remember to lock your screen and employ the clear desk policy.
* Always employ local procedures for escorting visitors.
* Remember end of day checks.

While a Defence site is the most secure place to conduct your work, do not assume that all controls are sufficient to stop threat actors from operating, such as malicious insiders. Do not assume everyone is abiding by the rules.

Complacency allows insiders to thrive.

### Working Offsite

**In Transit/In Public**

It is easier for external threats to access our information when it leaves the protection of our secure areas and enter into public spaces. Official information is especially vulnerable when it is in transit, or located in high public activity areas, such as airport lounges, transport hubs, etc. You have very little control over your environment and the set-up which can provide an unsafe place to do work.

**Conferences/Offsite meetings/F2F Training/Open Days**

You may be required to conduct official business in uncontrolled environments such as trade conferences, offsite meetings, training and open days. These environments are well known opportunities for FIS to gather information in a legitimate environment. Unlike when you are in transit where people may eavesdrop, in this situation you know that people are there to listen to what you have to show and tell.

Be careful of what you display as this may give away more information than you intended.

**Working From Home**

While you may have strong measures in place at home to stop basic criminals like thieves, when you bring Official information into your home you become a target for FIS.

This threat is very real. A security ‘attack’ will most likely occur via cyber means, or through the unintentional disclosure of Official information by yourself to a colleague, friend, or family member.

What can you do? Let the [Interactive Guide to Working From Home Securely guide your decision making.](https://ext.defence.gov.au/sites/default/files/media/ASA-Working-from-home-01.pdf)

**Overseas**

Intelligence services are most capable at home, where they control the environment and can draw upon a wide range of resources. You could be targeted at hotels, meetings, conferences, social events and in public places. Be extra vigilant of unsolicited approaches. Remember SOUP.

Ensure you are properly briefed in by your Security Officer for the destination/s you are travelling to. You should also go to [www.smartraveller.gov.au](http://www.smartraveller.gov.au) for country specific advice.

As an Australian clearance holder **you are required to advise your Security Officer of any official or private overseas travel**. Once your travel dates are known submit an AB644 form, Overseas Travel Briefing and Debriefing. Your Security Officer will organise a time with you to discuss the security implications of your travel. Make sure on your return you contact your Security Officer for a debrief.

[Return to Table of Contents](#Table_of_Contents)

## The insider and your responsibilities to report

### scenario – Team stand up

|  |  |  |
| --- | --- | --- |
| 1. The tradie has packed up and left, just in time for your daily team stand up. You are still at home so dial in using a Defence approved system. | 1. Lola: How was everyone’s weekend?   You: It was great! I bought myself a new car!  Lola: Oh fantastic! What did you get? | 1. You: I bought a new car, a blue one. It comes with all the bells and whistles. I got a great deal! Only $20,000! C:\Users\Developer\AppData\Local\Microsoft\Windows\INetCache\Content.Word\M3_Scenario_Team_YouDP.png |
| 1. Lola: You will have to show us when you are in the office next. Did you remember to report it to AGSVA?   You: What? What are you on about? | 1. Lola: Yeah, you have to. You have a clearance? It is your responsibility to do so.   You: Really? I didn’t know I needed to….  Lola: Well that can be your first task for today. |  |

### Self-Reporting

As an Australian Government security clearance holder you have a personal obligation to inform AGSVA of any significant changes to your personal circumstances.

You should report events that may affect your suitability to hold a security clearance, which can include:

* considerable changes to your financial situation such as large purchases, bank loans, or changes to household income;
* a change to your living situation such as a new address or co-habitant;
* a change in relationship status; or
* significant health changes that may have considerable impact to your employment or ability to work.

A full list of reportable changes can be found on the [AGSVA website](https://www1.defence.gov.au/security/clearances/applicants-holders/reporting-changes-in-circumstances).

**How to report**

You can make a Change of Circumstance report online via [AGSVA’s eVetting Portal](https://www1.defence.gov.au/security/clearances/applicants-holders/reporting-changes-in-circumstances).

**Why Report?**

An individual’s suitability to access classified information is based on an assessment of the individual’s overall integrity using the character traits such as honesty, trustworthiness, maturity and loyalty.

Over the course of time, it is normal for your personal circumstances to change. By self-reporting changes between periodic clearance revalidations your clearance can be continuously maintained, and any significant changes are less likely to be perceived as having been withheld; while also demonstrating your trustworthiness and understanding of your responsibilities as a clearance holder.

When Defence and AGSVA are aware of changes to your personal circumstance, it is less likely that these changes can be used as a lever by external threats (such as FIS and criminals) to coerce you. By self-reporting you are helping to protect yourself, your team, your project and Defence.

**Beware!** Providing false or misleading information during your clearance process could see you prosecuted under the *Espionage and Foreign Interference Act 2018* and prison time could be possible.

### The Insider Threat

**What is an insider?**

You will remember from Module 2 that an insider is a current or former employee with an intimate and legitimate knowledge of how Defence operates. They also happen to know about the security system and how to exploit potential vulnerabilities.

There are two types of insiders that Defence is concerned about, malicious and unintentional insiders.

* **Unintentional insiders** are trusted individuals who accidentally breech Defence security policy. Ignorance and apathy are not excuses, they are malicious in nature.
* **A malicious insider** is a trusted individual who wilfully and deliberately breaches the trust and access vested in them, compromising the security of Defence’s information.

**Beware!** Regardless of if it is an unintentional or malicious act, the action may still be considered an offence and therefore you may face disciplinary action or prosecution.

### Malicious Insider: Who Am I?

**Motivation**

Malicious insiders are motivated by gain. The gain could be monetary, ideological, revenge, desire for recognition or loyalty to others. Some malicious insiders could be coerced by external threat actors.

**Incidents**

The different kinds of incidents which a malicious insider might conduct include;

* Unauthorised disclosure of Official information
* Process corruption
* Facilitation of threat access to assets
* Physical/electronic sabotage.

**Warning Signs**

How to recognise the warning signs for malicious insider activity?

The Centre for the Protection of National Infrastructure (CPNI) insider data collection study shows that there are three key factors that you need to recognise that may indicate a potential malicious insider:

* Personality traits (e.g. manipulative, emotionally unstable, unethical, low self-esteem, disgruntled)
* Lifestyle/circumstantial vulnerabilities (e.g. serious financial problems, substance abuse, gambling problems, recent negative life events, loss of loved one, relationship breakdown)
* Workplace behaviours (e.g. poor work attitude, unauthorised access to assets, commits security incidents).

**Note:** It is important that the factors described above are not taken out of context and are not used as a means to profile or discriminate against colleagues who display some of those behaviours.

**Report or seek advice**

If you observe or are concerned about your colleagues behaviours, it is essential that you talk to your Commander/Manager or Security Officer.

### don’t assume or ignore - Five Don’ts

For Everyone:

1. Don’t assume that malicious insiders don’t exist, and don’t operate in your area.
2. Don’t assume security controls will stop insiders. Policies and processes are not always followed, especially in areas of poor security culture.
3. Don’t assume the initial security clearance process solves the insider problem. People change over time.
4. Don’t ignore the warning signs. If you see something unusual, report it to your Commander/Manager ASAP.

For Commanders/Managers;

1. Don’t ignore morale issues. Creating a harmonious work environment where people want to work in your team reduces animosity and aids in suppressing malicious activity.

**Case Studies:**

#### The Secret Affair

Denise\* recently underwent a Positive Vetting (PV) clearance. About a month after having her clearance granted, Denise had a sexual relationship with a colleague, whilst married. Terrified that her husband would find out, Denise kept this a secret from everyone and did not report the affair to AGSVA.

Unfortunately the boyfriend wasn’t so discreet and started bragging to other colleagues, one of whom advised his Security Officer. The Security Officer submitted an SVA004 Change of Circumstances to AGSVA who contacted Denise. Denise denied the affair initially, then felt guilty so she contacted AGSVA to advise that she had been in another ‘relationship’. AGSVA could have potentially mitigated the risk through a discussion with Denise about the potential vulnerability her relationship had exposed her to.

By not reporting the extra marital affair, and denying it when questioned Denise had displayed a lack of integrity that put her clearance at risk, and an assessment of her suitability to hold a security clearance was undertaken. Not to mention, lying to AGSVA could see Denise prosecuted under the *Espionage and Foreign Interference Act 2018*.

#### Drugs at the Party

Brian\* was a pilot in the RAAF who was granted a PV in 2012, and attended his school reunion in 2018. He enjoyed catching up with his old friends at the event, and there was plenty of drinking and merriment. Brian took part enthusiastically as he was on leave for the fortnight.

During the course of the evening Brian noticed several people disappearing into the toilets in small groups, and shortly afterwards one of the women persuaded him to join her and another woman in doing a line of cocaine. At first Brian refused, but when the women good-naturedly teased him, he decided to throw caution to the wind and took the drug. Although he felt terrible and guilty afterwards he decided not to say anything for fear of this impacting his career.

As a member of the Australian Defence Force, which has a zero tolerance for drug taking, and a holder of a Security Clearance, he had breached the *Defence Force Discipline Act 1982* and responsibilities as an employee.

Some weeks later Brian ran into a colleague and his wife. The wife recognised Brian from the reunion event and told her husband that she’d witnessed Brian taking cocaine. The colleague reported this to his Security Officer who advised ASGVA and Brian’s Commanding Officer. Brian was drug-tested and traces of cocaine were found in his system.

Brian was stood down pending an investigation and an assessment of his suitability to hold a security clearance was undertaken. During the assessment, it was identified that Brian’s decision not to disclose the drug taking compounded the suitability concerns as this indicated deceptive, dishonest behaviour.

[Return to Table of Contents](#Table_of_Contents)

## Cyber: Anywhere, Anytime

### scenario – The Army Day of Cyber video

|  |  |  |
| --- | --- | --- |
| 1. To finish off the team stand up your manager asks everyone to watch [The Army Day of Cyber](https://objcdc1/id:BN18621382/document/versions/published) video before tomorrow. | 1. You: What is it about?   Lola: It is about cyber security. You wouldn’t believe what can happen! C:\Users\Developer\AppData\Local\Microsoft\Windows\INetCache\Content.Word\M3_Scenario_Team_LolaDP.png | |
| Embed Army Day of Cyber Video to watch | | |
| 1. As you sign off from the meeting you think, “pfft that wouldn’t happen to me!” Time to catch up on your emails. You are scrolling through and find an email regarding your new car warranty. | 1. It is a little odd because you were not expecting to receive it. I has a deal for extended warranty asking you to click for further details. | 1. You decide to take a better look, you are about to click the link but hesitate... |

### The global threat of cyber

The use of social media, apps and other online services have made our lives more convenient, both at work and at home. Unfortunately this has also made it convenient for threat actors to infiltrate our lives and socially engineer an attack from anywhere in the world.

Cyber attacks are more common than you might think. According to the ACSC Annual Cyber Threat Report July 2019 to June 2020, 164 successful or attempted attacks are reported on average per day, approximately one every 10 minutes. And that is only what is reported, this number is likely much higher! Defence has a strong cyber security system to protect against attacks however this can only protect against what is known. Cyber criminals are developing new tactics every day to bypass these controls.

Let us now add the human factor. Many cyber attacks require a human action to initiate the attack, and cyber criminals are getting very good at tricking us. In 2019 Australian’s lost over $634 million due to scams with the top three being business email compromise, investment and dating/romance scams. While the true cost of cybercrime to the Australian economy is difficult to quantify, industry estimates have previously placed cyber security incidents as high as $29 billion annually.

**You are part of cyber system, you could be our biggest vulnerability.**

### You and Your Family

To be a responsible cyber user it is important that you maintain good awareness of cyber security. Easy ways you can do this are by registering with the [ACSC Alert Service for individuals and families](https://www.cyber.gov.au/acsc/register/individuals-and-families) or by following the Australian Cyber Security Centre on Facebook. These will provide you with easy tips and information to help keep you cyber aware. This information will help you to remain vigilant and proactive when using technology.

Remember, your security responsibilities do not end when you log off or leave the worksite. With 80% of Australians online, the boundaries between peoples’ personal and professional lives are blurring. Cyber is a 24/7 issue and not only impacts you, it impacts your family, your children and your friends.

**Did You Know?** Cyber awareness is so important that it is now part of The Australian Curriculum. Why don’t you have a chat to your family, especially those with children when you get home? To help guide your conversation, check out the [ACSC website](https://www.cyber.gov.au/acsc/individuals-and-families) which provides resources for information and [resources](https://www.cyber.gov.au/acsc/view-all-content/guidance/family-resources) to assist you and your family at home.

### **How can we be compromised?**

**Cyber-attacks** are becoming sophisticated in their look and content, they can be difficult to spot as they can appear to come from legitimate sources. There are many methods threat actors may use in an attempt to compromise you. These include;

* **Phishing** - the process of deceiving recipients into clicking links or sharing sensitive information with an unknown third party. Phishing can occur via all electronic media including email, SMS and social media messaging.
* **Spear-Phishing** - is targeted phishing. The email is socially engineered and will often contain a sender address and possibly content which appears to be legitimate.
* **Spam** - any unsolicited commercial email (junk mail).
* **Malware** (short for 'malicious software') - is the term used to refer to any type of code or program that is used for a malicious purpose.

Threat actors can target anyone at home or at work. They can use fake links designed to trick you into providing your credentials or fake attachments designed to download malware onto your device. These are usually an attempt to steal your money or access to information. Your information can be stolen or extorted through your account or system credentials, holding your accounts or computer to ransom, or by installing programs which could collect information without your knowledge.

### How to Avoid Compromise - Prevention

To avoid compromise:

* Only use Defence accredited systems to access Official information.
* Never plug a USB into a Defence network unless approved by Defence (mobile phone and watch chargers are not approved, even if they have been provided by Defence). USB devices (including watch and phone chargers) can be infected with malware at any time, even during manufacturing, and you might never know. **The Defence network is not to be used as a charging station.**
* Keep your operating systems (Windows/Mac OS/Linux) up to date.
* Keep your virus protection up to date and run scans regularly.
* Strong passphrases are more secure than passwords. If you would like more information on passphrases and passphrase protection you can head to the [ACSC website.](https://www.cyber.gov.au/acsc/view-all-content/publications/creating-strong-passphrases)
* Do not use personal email, social media or personal storage devices for work information.
* Protect your Defence issued Portable Electronic Device (PEDs) as per the DSPF and relevant SOPs.
* Never connect your Defence PED to a public WiFi network.

**Are You Aware?** Defence issued PEDs must be procured through the CIOG Log a Job Service. As the person ordering the asset, it is important that you understand your security and custodianship obligations. You remain responsible for the asset until a change of custodian form has been submitted and approved.

### How to Recognise and Report

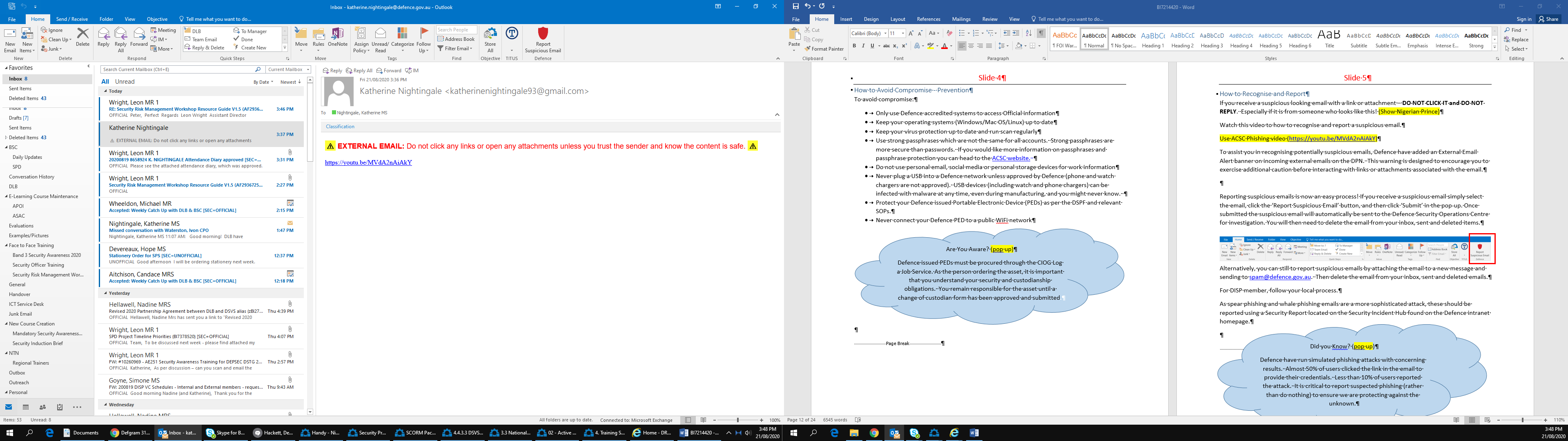
Watch this [ACSC Phishing](https://extd8.govcms.gov.au/sites/default/files/2021-01/ACSC-How-to-identify-phishing-messages.mp4) video on how to recognise and report a suspicious email.

If you receive a suspicious looking email with a link or attachment – **DO NOT CLICK IT and DO NOT REPLY**.

To assist you in recognising potentially suspicious emails, Defence have added an External Email Alert banner on incoming external emails on the DPN. This warning is designed to encourage you to exercise additional caution before interacting with links or attachments associated with the email.

**Reporting suspicious emails is an easy process!**

If you receive a suspicious email simply select the email, click the ‘Report Suspicious Email’ button, and then click ‘Submit’ in the pop-up. Once submitted the suspicious email will automatically be sent to the Defence Security Operations Centre for investigation. You will then need to delete the email from your inbox, sent and deleted items.



Alternatively, you can still report suspicious emails by attaching the email to a new message and sending to [spam@defence.gov.au](mailto:spam@defence.gov.au). Then delete the email from your inbox, sent and deleted emails.

As spear phishing emails are a more sophisticated attack, they should be reported using a Security Report located on the Security Incident Hub found on the Defence intranet homepage.

**Note:** For DISP members, follow your local process.

**Did you know?** Defence have run simulated phishing attacks with concerning results. Almost 50% of users clicked the link in the email to provide their credentials. Less than 10% of users reported the attack. It is critical to report suspected phishing (rather than just delete) to ensure we are protecting against the unknown.

[Return to Table of Contents](#Table_of_Contents)

## Be social media savvy

### scenario – Social media Browsing

|  |  |  |
| --- | --- | --- |
| 1. Having seen the video you decided not to click the link. There were too many red flags and you report it using the report suspicious email button. | 1. After a big morning you are very hungry, time for lunch. | 1. While you are eating you decide to do a bit of social media browsing on your personal phone. |

### Your social media footprint

**Ever thought about what you are posting? Social media** is a great way to keep in touch with family and friends but have you ever thought about the information you are posting on your social media accounts?

**Some questions to think about:**

* How much are you telling people with your online presence?
* Can someone build a picture of your life from your online information?
* Would you feel comfortable telling complete strangers where you live, who your family are, what your daily routines are, where you work, etc?

You have complete control over your social media footprint through what you are posting online.

what do threat actors look for?

Threats actors seeking to gather information about you and Defence are increasing. They use information collected on social media to craft approaches to individuals for targeting and cultivation. Aggregation of information on social media can add up and reveal more about you and Defence than you intended.

What information do threat actors look for on social media?

|  |  |  |
| --- | --- | --- |
| **Work Profiles**: What you know and what you have access to - capabilities, equipment, intelligence, technologies etc. (e.g. what you would find on LinkedIn) | **Personal Profiles**: Who you are - information that could be used against you such as family issues, financial problems, emotional stresses, ego, extreme views etc. (e.g. Facebook, dating apps, etc.) | **Pattern of Life**: What you do & where you go – details about your routines, habits and movements (e.g. Facebook, Instagram, Twitter, etc.) |

**ACTIVITY:** Put yourself in the shoes of a threat actor. What work and personal information can you find out about Joe Bloggs, and can you build any patterns of life?

Watch this [video](https://ext.defence.gov.au/security/resources#security-awareness) on how threat actors can use information found on social media this to conduct a suspicious approach.

suspicious approach

Have you encountered someone online who was not who they seemed to be? Maybe your social media profile has given away too much information and someone has taken an interest in you.

Suspicious approaches are now more common and represent a high risk to Defence and defence industry. To counter this at the national level, ASIO have developed the [Think Before You Link](javascript:var%20newWnd=ObjLayerActionGoToNewWindow('https://www.asio.gov.au/TBYL.html','Trivantis_','width=1025,height=701,scrollbars=1,resizable=1,menubar=1,toolbar=1,location=1,status=1');) campaign.

Please be aware that if you intend to watch the videos on the ASIO Outreach site, they are in You Tube and won’t work on the DPN. We have saved the videos on the [Course Resource page](https://ext.defence.gov.au/security/resources#security-awareness).

### scenario – Reflection

|  |  |  |
| --- | --- | --- |
| 1. The time has come to finish up for the day. As you are closing everything down you reflect on the conversation you had with the tradesperson earlier in the day. | 1. Why were they so interested in your work and how did they know you were on that project? | 1. You decide to write down the details of the incident and send a calendar invitation to your Security Officer to discuss it tomorrow. |
| 1. You log off DREAMS and because you only accessed soft copy information you do not need to worry about securing any documents. | 1. You now reflect on all the security things you looked at today. You realise that if you follow all of these you reduce the likelihood of a security incident occurring | 1. You now feel comfortable that you are not a security vulnerability. |

[Return to Table of Contents](#Table_of_Contents)

## M3 | Knowledge Check

Question 1

**To help us to identify a potential approach of concern we use the acronym SOUP. What does this stand for?**

Select the correct answer.

* Suspicious occurrences, Ongoing contact, Useful information, Persistent questions
* Sad, Ongoing contact, Unusual incidents, Persistent approaches or questioning
* Suspicious occurrences, Ongoing contact, Unusual incidents, Persistent approaches or questioning
* Suspicious occurrence, Ongoing contact, Unusual incidents, Party personality

Question 2

**Your colleague is organising a team meeting to discuss OFFICAL Defence information via Zoom. Your response is;**

Select the correct answers.

* Accept the invitation
* Ask why a Defence approved system is not being used?

Question 3

Sarah has held an Australia Government security clearance for two years. Since her clearance was granted she has finally saved enough to buy a house and has purchased a three bedroom property which she has a mortgage on. Her partner has moved in, they got married and bought two dogs. Sarah has purchased a new car took one month off to road trip around the eastern states of Australia.

**What changes Sarah would need to advise to AGSVA?**

Select the correct answers.

* Purchase of property
* Change in savings and new bank loan
* House has three bedrooms
* Partner has moved in
* Marriage
* Ordered a pizza
* New car
* Time off work to road trip in Australia
* Change in contact details
* Joined a gym
* Started at university
* Watched a movie

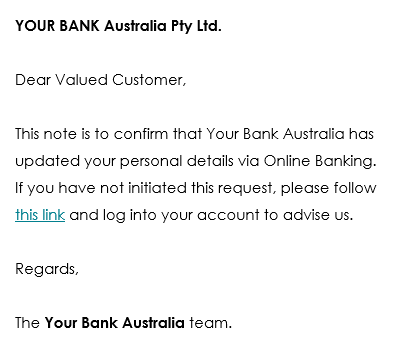
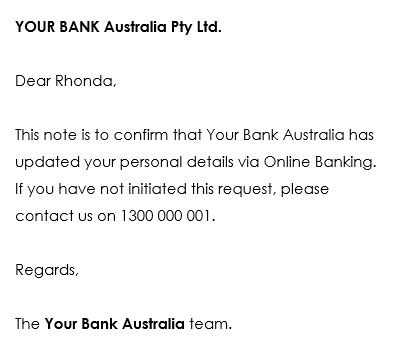
Question 4

Have you submitted all your change of circumstances to AGSVA since gaining a clearance or your last revalidation?

* Yes – I have reported all my change of circumstances
* No – I have reportable change of circumstances but haven’t got around to it
* No – I have reportable change of circumstances but did not know I had to report them
* No – I have not had any reportable change of circumstances

Question 5

**Identify which of these emails is a phishing email?**

**A  B **

Select the correct answer.

* A
* B

### question 6

Threat actors collect information found on social media to craft approaches.

Information they may be seeking include:

|  |  |  |
| --- | --- | --- |
| Information | Match the pairs  (e.g. 1 = A) | Example |
| 1. Work profiles | 1 = A | 1. What you know and what you have access to |
| 1. Personal profiles | 2 = B | 1. Who you are. |
| 1. Patterns of life | 3 = C | 1. What you do and where you go |

Question 6

Foreign Intelligence Services are most comfortable operating in what type of environment?

Select the correct answers

* Within your workplace
* In uncontrolled spaces such as offsite conferences, trade shows and public spaces
* Outside of Australia, within their own backyard.
* Near you home, physically
* Online

Knowledge Check COMPLETE

Well done, you have completed the knowledge check for Module 3.

[Return to Table of Contents](#Table_of_Contents)

## M3 | Module Summary & Commitments

### MODULE SUMMARY

Below is a summary of what you learnt in this module:

1. You are required to maintain your security clearance through **self-reporting.**
2. With our work environments now being more flexible it is important you need to **be aware of your surroundings** at all times, especially when in uncontrolled spaces and when handling and discussing Official information
3. **Recognise and report:**
   1. unusual behaviours (to your commander/manager or Security Officer);
   2. suspicious emails by simply clicking on ‘Report Suspicious Email’ button in Outlook; or
   3. alternatively, to report suspicious emails or contacts, you can email [spam@defence.gov.au](mailto:spam@defence.gov.au)
4. The importance of cyber security and being social media smart:
   1. You are part of our cyber system, **you could be our biggest vulnerability**
   2. When working offsite, a security ‘attack’ will most likely occur via cyber means, or through unintentional disclosure of Official information by yourself to a colleague, friend, or family member
   3. Aggregation of information on social media can add up and reveal more about you and Defence than you intended

### M3 | YOUR COMMITMENTS:

Throughout this course you’ll make a number of commitments designed to encourage you to make good Security choices. These commitments will form part of your Completion Certificate.

You are required to tick the commitments and sign (below) in each module.

|  |  |
| --- | --- |
|  | I will be security aware of my surroundings at all times, especially when handling and communicating official information. |
|  | **I will commit to maintaining my clearance through self-reporting any change of circumstances.** |
|  | **I will commit to reporting any unusual behaviours, suspicious emails and contacts.** |
|  | **I will remain cyber vigilant and being social media smart.** |



### MODULE COMPLETE

**Well done, you have completed Module 3 | How to prevent security incidents.**

The next module in this course is **Module 4 | Responding to security incidents.**

[Return to Table of Contents](#Table_of_Contents)

# MODULE 4 | **Responding to security incidents**

## M4 | Module overview

This module covers how to identify, inform and respond to security incidents.

Module objectives:

1. How to identify and record a security incident
2. Informing your Commander/Manager or Security Officer of the situation
3. Responding to security incidents

[Return to Table of Contents](#Table_of_Contents)

## identifyING a security incident

### What is a security incident?

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

* Fails to meet the expected outcomes of the DSPF or compromises Defence’s protective security arrangements; and
* Has resulted in, or has the potential to result in loss, damage, disclosure, or harm to Defence’s information, assets and/or personnel.

If you observe a security incident occurring (or has occurred), it is important that you respond appropriately and immediately. The best thing you can do is **IDENTIFY & INFORM.**

### Identify the incident and record

During this course you have learnt how to identify vulnerabilities, suspicious activities and things that look out of the ordinary. It is essential that you record in detail everything that you observe.

Look at the following scenario and record as much detail as possible on a piece of paper – Good luck.

Caller: Hey Brian, it’s Steve calling from Russell Offices. I gotta be quick before someone hears…I have access to the secured files. I’ll send login details COB today 4th Feb. Copy everything tonight! I’ll delete any evidence and login details tomorrow. I’ll call later when it is safe to speak.

What could you record?

* Name?
* Where they were from?
* Gender?
* Physical characteristics?
* Time and date?
* Place (location)?
* What were the circumstances?
* What was said?

[Return to Table of Contents](#Table_of_Contents)

## Inform your Commander/Manager or Security Officer of the situation

Now that you have identified and recorded your observations, it is imperative that you inform your Commander/Manager or Security Officer immediately. They will manage the security incident until it has been resolved, including reporting it through to the appropriate authorities.

If your Commander/Manager or Security Officer are unavailable – you are obligated to report via a Security Report. For information on making a Security Report see:

* the [Incident Reporting Hub](http://drnet/AssociateSecretary/security/services/Pages/incidents-reporting.aspx) (for those with DPN access) or
* the [Make a Security Report](https://www1.defence.gov.au/security/industry/make-security-report) page (on the DISP website for industry).

Do not forget about the other forms of reporting you looked at in Module 3; Change of Circumstance and Cyber incidents.

**Don’t consider informing and reporting as snitching, dobbing or creating trouble**.

Informing will protect you and your team in the long run. Imagine if you didn’t inform at the earliest opportunity and the security incident got LARGER AND LARGER and impacted lives, finances and your employment prospects in the future. How would you feel now?

The benefits of informing and reporting:

* Allows Defence to understand/become aware of actual threats, this in turn allows us to respond
* Identifies vulnerabilities in the security system
* It allows decision makers to formulate recommendations and actions
* May shape new policies and response measures
* The knowledge that you did the right thing!

[Return to Table of Contents](#Table_of_Contents)

## Emergency response to a violent security incident

You may not have enough time to respond how you would ordinarily to a security incident due to its violent nature. In order to save life, injury and other forms of harm – you need to understand and respond in accordance with your local Emergency Procedures.

All areas are to have Emergency Procedures in place to respond to the threat of violent acts. You will find these in your local procedures. Your Commanders/Managers should be briefing you on these procedures on induction to Defence and on an annual basis. If you are escorting visitors to your area you need to brief them on the same procedures on the off chance that something may occur - it is a duty of care.

Emergency procedures on a Defence base will be informed by the SAFEBASE alert system. There are three levels AWARE, ALERT & ACT as per diagram and the table below.

Safebase Security Alert System Diagram. Aware - Security Aware / Normal business
Alert - Increased security / restricted business
Act - Follow emergency procedures

|  |  |
| --- | --- |
| **SAFEBASE Security Alert System – Guidance for individuals** | |
| Alert level | What the alert levels mean to you |
| **Aware** | **Understand**: Defence has no knowledge of a threat to my establishment but I should be aware of my security responsibilities - and expect normal business.  **How should I behave?**   * 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** | **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.  **How should I behave?**   * 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** | **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  **How should I behave?**   * 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. |

[Return to Table of Contents](#Table_of_Contents)

## M4 | Knowledge Check

Question 1

**If you observe a security incident occurring (or has occurred), the best thing you can do is:**

Select the correct answer.

* **IDENTIFY & INFORM** by recording in detail everything that you observe
* **DETECT & NOTIFY** by calling the Australian Federal Police to report
* **CAPTURE & DETAIN** the suspected threats

Question 2

**What are the benefits of reporting a Security Incident?**

Select the correct answers.

* Enables Defence to understand and respond to threats
* May shape new policies and response measures
* Identifies vulnerabilities in the security system
* It allows decision makers to formulate recommendations and actions
* The knowledge that you did the right thing!
* Remuneration and rewards depending on the incident
* Possibility in promotion of rank or role

Question 3

**Have you received a briefing from your Commander/Manager or Security Officer regarding local Emergency Procedures within the last 12 months?**

* Yes
* No

[Return to Table of Contents](#Table_of_Contents)

## M4 | Module Summary & Commitments

### MODULE SUMMARY

Below is a summary of what you learnt in this module:

1. If you observe a security incident occurring (or has occurred), the best thing you can do is **IDENTIFY & INFORM** by **recording in detail** everything that you observe.
2. If you have identified and recorded your observations, it is imperative that you inform your Commander/Manager or Security Officer immediately. If this is not possible, you are obligated to report via a Security Report (Incident Reporting Hub for those with DPN access) or the Make a Security Report page on the DISP website for industry).
3. All areas are to have Emergency Procedures in place to respond to the threat of violent acts. You will find these in your local procedures

### M4 | YOUR COMMITMENTS:

Throughout this course you’ll make a number of commitments designed to encourage you to make good Security choices. These commitments will form part of your Completion Certificate.

You are required to tick the commitments and sign (below) in each module.

|  |  |
| --- | --- |
|  | I will inform my Commander/Manager or Security Officer of any Security incident I observe. |



### MODULE COMPLETE

**Well done, you have completed Module 4 | Responding to security incidents.**

The next module in this course is **Module 5 | Where to go for your security needs.**

[Return to Table of Contents](#Table_of_Contents)

# MODULE 5 | **Where to go for your security needs**

## Security Officers

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

Your local Security Officer has been trained by DS&VS to:

* Advise you on your security needs especially the implementation of the DSPF
* Promote positive security culture and awareness
* Provide you with local security briefings
* Provide you with security administrative support
* Co-ordinating and assisting you through the Clearance process
* Assist you with the security reporting process

If your Security Officer can’t find the answer they can contact 1800 DEFENCE or other security authorities on your behalf.

Do you know who your local Security Officer is? If not, speak to your Commander or Manager to find out. You can search your local Security Officer using the Defence Corporate Directory search engine.

**Your Security Officer is a valuable resource for you and your team! Use them.**

[Return to Table of Contents](#Table_of_Contents)

## The Security Portal

Before contacting your Security Officer for advice why don’t you look up the information yourself? DS&VS have a range of product to support you and your security needs.

**Access the Security Portal via the DPN – DRNet Home > Security.**

Visit the Security portal homepage and discover:

* DSPF
* Security News (Bi- monthly newsletter keeping you up to date with the latest security advice and tools)
* Training and Awareness products (Do you need self-help tools, security awareness and briefing products, fact sheets, or do you require further security training)
* Threat products (understand your local environment)
* Security Risk Management (Tools, templates and advice to assist)
* Toolkit of security forms, tools and templates
* AGSVA (to find out more about the security clearance process)

**Access the Security Portal externally**

If you are a defence industry employee and do not have DPN access, you can visit the [Defence Industry Security Program website](https://www1.defence.gov.au/security/industry).

Here you will find:

* DSPF
* DISP Information:
  + How to Apply
  + Eligibility and Suitability
  + Maintaining Membership
  + Assurance
  + FAQs
  + Contacts
* Resources (Forms, policies and standards, guides and fact sheets, and Security Officer toolkit)
* Training (What security training is available and how to access it)

If you can’t find what you need chat to your local Security Officer!

[Return to Table of Contents](#Table_of_Contents)

## Course COMPLETE

**Well done, you have completed the Annual Security Awareness Course!**



[Return to Table of Contents](#Table_of_Contents)

Throughout the course you made commitments regarding your security behavior. We recommend that you print or download your commitment certificate and reflect on a regular basis.

Supervisors – please use the commitment certificate as a reference during any performance and development discussions with your employees.