Australian Government
Department of Defence

Defence Security and Vetting Service
Enabling Defence capability through security services

Security Awareness eLearning content

June 2019 - version 3.0

Accessible version

This PDF has been designed for accessibility purposes and access to the assessment is subject to meeting the requirements outlined in Annex A of this document. If you do not meet the requirements, you will have to complete the mouse or keyboard version. This will include reviewing the complete course content before attempting the assessment.

We are working towards making our products more accessible. If you have any feedback or suggestions, please email them to DSVS.Skilling@defence.gov.au with "Security Awareness course feedback" in the subject line.

Who to contact for further information

This course was developed by Building Security Capability section within the Defence Security and Vetting Service with the assistance of the Defence Learning Branch.

Requests and enquiries should be addressed to:
Building Security Capability Section
Defence Security and Vetting Service
CP3-3
PO Box 7951
Canberra BC ACT 2610
DSVS.Skilling@defence.gov.au

Copyright details

Introduction

Security is everybody's business

Our national security relies on us understanding and acting on our security responsibilities.

This course has been developed to provide an overview of security and introduce your '8 Security Essentials' - core personal security responsibilities designed to promote a consistent Defence security culture.

The term “security” may evoke mental images of contracted guards or specialists working to protect technical systems, or unknown specialists working on secret business to protect from the unknown. In fact no matter what rank or position you hold, every member of Defence plays an integral role in maintaining Defence's security.

As a member of Defence you are entrusted with official information, which you have an obligation to protect. You will learn more about your obligations and how to meet them through this course. By following the guidance provided you will be helping to make Defence more secure through meeting your own security responsibilities.

The 8 Security Essentials

Security Essential 1. Complete your security training annually - apply it in your workplace

You have already taken the first step in doing the mandatory security awareness course. Did you know that there are five other security courses available for you to complete. These are:

1. **Basic Document Handling (BDH)**

   For all who access official information marked PROTECTED and below as part of their duties. It is recommended that you undertake this course every two years.

2. **Classified Document Handling (CDH)**

   For all who access official information marked CONFIDENTIAL and above as part of their duties. It is recommended that you undertake this course every two years.

3. **Security Officer (SO)**

   APS, ADF & Defence Industry Security Program (DISP) Security Officers to complete on appointment to SO role and every three years thereafter.

4. **Security Risk Management (SRM)**

   Workshop recommended for Defence staff with a requirement to conduct Base or Security Planning, capability development or project work. Commanders and Managers are also strongly encouraged to complete this course.

5. Cyber Security Awareness

Recommended for all users of Defence Information Communications Technology (ICT).

For further information, visit the Defence Security Training & Awareness webpage on the Security Portal.

Security Essential 2. Enforce the need-to-know – Protect official information

Correct access to official information ensures a secure Defence. If Defence does not protect its own information and that received from external parties, its ability to function in support of the Government will be undermined.

Defence expects that suitable controls be applied to official information to ensure it is protected. Exercising the need-to-know principle is one such control. Classified information must only be released to, and accessed by, people with an appropriate level of clearance and a need-to-know.

Knowledge of how to handle, store, apply protective markings, register, physically transfer and dispose of official information, can be attained from undertaking the Document Handling Courses. It is recommended that you undertake the appropriate course every two years.

Security Essential 3. Report all security concerns and incidents

Reporting security incidents and helping security investigations are the responsibility of us all. Defence's ability to detect, assess and mitigate security vulnerabilities depends upon accurate, timely and consistent reporting of all security incidents from across Defence.

There are three types of security incidents: Reportable Major Security Incidents, Major Security Incidents and Minor Security Incidents. Along with the XP168 contact reporting scheme, the Security Incident Centre deal with thousands of security incidents annually.

The information collected and analysed in security incidents aids Defence in strengthening its defensive posture against insider threats, Foreign Intelligence Services and other threat types.

Forms for reporting security concerns and incidents are:

- **XP188 Security Incident Report** - to be submitted by personnel and/or Security Officers to report security incidents if they suspect a breach of security.

- **XP168 Report of Contact of Security Concern** - to be submitted by personnel and Security Officers to report suspicious, ongoing, unusual or persistent (SOUP) contact by unknown persons, including suspected malicious insiders.

Module 2 provides further information on what security incidents and suspicious contacts are, and how to go about reporting them.

Security Essential 4. Maintain your security clearance – report personal changes to AGSVA

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

As a clearance holder, you should report changes to your personal situation (through the SVA003 Change of Circumstances Notification form), as well as report significant changes in the personal circumstances of others where you believe there to be an implication for security (through the SVA004 Security Officer / Manager Change of Circumstances Report).

Forms for reporting change of circumstances are:

- **SVA003 Change of Circumstances Notification** - to be submitted by individuals reporting changes in their circumstances for security clearance purposes.

- **SVA004 Change of Circumstances Report** - to be submitted by the manager or Security Officer reporting change of circumstances or behavioural change of personnel.

Module 4 provides further information on how to report personal changes to the Australian Government Security Vetting Agency (AGSVA).

Security Essential 5. Practice good cyber security

Ensuring that you keep security front of mind when working with technology is important in keeping Defence secure. Common types of cybercrime include hacking, scams, identity theft and attacks on computer systems.

Be wary of where you are allowed to take Portable Electronic Devices, report suspicious emails (phishing or spear phishing) and NEVER plug an unauthorised device (such as your phone) into the Defence Network.

CIOG have a Cyber Security Awareness course (available on CAMPUS) which covers identifying and combatting socially engineered emails.

Module 6 provides further information on what you need to do if you encounter socially engineered emails and how to report them.

Security Essential 6. Be secure online – follow Defence social media policy

Be proud to be part of Defence, but be wary of who may read your posts and how they may be used. Use of social media and digital communication is increasing, but Defence staff must be cognisant that publishing online constitutes public comment, and use of digital channels in both an official and private capacity must be consistent with the values and information posture of the organisation.

Digital content is commonly used to coordinate and/or publicise Defence activities, but must be done so with channels appropriate to the sensitivity of the information needing to be published.

Module 6 provides further information on Defence's social media policy.

Security Essential 7. Understand security threats and risks

In Defence, we operate in an environment where our activities, our information and our people, come under great scrutiny. Defence specifies threat types and provides the latest intelligence on threat sources, modus operandi and past attacks. Threats include the insider threat, Foreign Intelligence Services and Issue-Motivated Groups.

DS&VS works with other security intelligence agencies and can provide intelligence, based on the need, to activities, projects and bases in order to inform effective security planning. Security Risk Management is the process conducted in Defence for that security planning.

There is a Security Risk Management Workshop available which provides participants with knowledge on how to apply security risk principles in a Defence context. The one-day workshop is aimed at those involved in security planning – whether it be for base and asset protection or for event and project planning. You can nominate for it via CAMPUS.

Module 2 contains further information on the security threats that Defence faces and what you can do if you encounter them.

Security Essential 8. Know your Security Officer and where to get help

Defence has security specialists embedded throughout the organisation in order to achieve good security results. The frontline security professional most people are familiar with are Security Officers – if you have a security clearance, you will have a Security Officer. Get to know yours, they provide immediate security advice to personnel and to management, as well as aiding clearance processes, ensure security reporting occurs, facilitate security audits and much more.

While there is in place this security professional community, remember – security is everybody's business. The new principles framework for security policy is written with access in mind so that everyone can easily read their obligations and understand.

Other resources

Other resources where you can access security advice include:

- Defence Security Portal on the left menu of the DPN homepage under 'Security'
- 1800DEFENCE and yourcustomer.service@defence.gov.au
- Executive Security Advisers from the resources menu on the policy page of the Defence Security Portal
- Defence Online Services Domain (DOSD) Security Portal for Defence Industry Security Program (DISP) members
- ServiceConnect for links to DS&VS services

SAFEBASE - The New Security Alert System

The new SAFEBASE system came into effect on 25 March 2019 and has been simplified to three alert levels:

- **Aware:** Security aware – Normal business.
- **Alert:** Increased security – Restricted business.
- **Act:** Follow emergency procedures.

What the new SAFEBASE is:

- An alert system communicating the threat of a violent act on Defence premises.
- Three tiers - base level of AWARE, mid-level of ALERT, highest level of ACT.
- Used at all Defence premises across Australia.
- A system where each SAFEBASE level informs security measures to prepare, deter or respond to an act of violence.
- Set nationally by the Chief Security Officer and reviewed at set times.
- Used locally. See your Base Manager or Senior ADF Officer for advice about local arrangements and your Security Management Plan.

What the new SAFEBASE is not:

- It is NOT an all hazards alert system (it is not about environmental hazards like cyclones or bushfires, or emergencies like gas leaks or water shortages)
- It does NOT align to the old 5-tier system (AWARE does not equate to BRAVO).

Your responsibilities at each new SAFEBASE level can be found in Module 2 of this course.

Transition from the Defence Security Manual (DSM) to the Defence Security Principles Framework (DSPF)

Historically Defence security policy used terms like 'must' and 'should' to indicate security obligations. In July 2018, Defence moved to a security risk management approach by replacing the Defence Security Manual (DSM) with the Defence Security Principles Framework (DSPF). This principles-based approach is considered by Government to be best practice.

The DSPF gives Defence more flexibility and agility by allowing areas to meet the intent of security, rather than simply complying with a manual.

A risk managed approach increases responsiveness to and awareness of risks, as well as empowering staff to take the appropriate and measured steps to secure their environment.

The risk management model is a process of:

- Identifying risks,
- Assessing risks, and
- Taking steps to reduce risks to an acceptable level.

The DSPF, in addition to policy, has support pages containing terminology guides and other resources to assist you in applying the DSPF. Visit the *Policy Tab* on the Security Portal for more information.

Module 1: What is security?

At the end of this module, you will be able to:

- describe the Security-in-Depth principle
- demonstrate an awareness of the Defence Security Regime
- list the key security roles in Defence.

What is security?

Security is the protection and preservation of an organisation's assets, including its people, property, information and activities, from sources of harm.

Defence has five key security objectives:

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

You can get further information about how your area does security by reading your unit's Security Standing Orders and/or talking to your Security Officer.

Why is security important?

Security incidents can be the result of an intentional attack such as espionage, though the overwhelming majority of incidents are actually the result of negligence and poor security practices in the workplace.

It is important for all Defence personnel to realise that the disclosure of sensitive or classified information can be damaging, possibly catastrophic —even if you didn't mean it!

If such information is disclosed—either through accident, negligence or deliberate action—it could risk the success of Defence operations and endanger the lives of Defence personnel.

Capability edge can be lost, dollars can be wasted and people can be put at risk as a result of poor security!

That is why it is important for you to follow security policies and procedures at all times.

Defence Security Regime

The Defence Security Regime is dictated by legislation, which is further supported by policy. Both outline your responsibilities as a Defence employee.

Legislation

Legislation is borne out of the enactment of law by Parliament. It is the dominant reference and is enforced by various law enforcement agencies. Consequences are varied but can include imprisonment.

Policy

Policy is more flexible: it is guided by legislation and developed to provide more specific departmental guidance. It also provides staff with expectations of conduct, behaviours and responsibilities that the Department can enforce.

Breaches of policy can incur censure, dismissal and potential referral to authorities for further investigation should the need arise.

Defence Security Regime: legislation

The Defence Security Regime consists of legislation that outlines your responsibilities as a Defence employee. The key pieces of legislation are detailed below.

Crimes Act 1914 and Criminal Code Act 1995

The Crimes Act 1914 and Criminal Code Act 1995 establish offences in relation to the unauthorised disclosure of sensitive Commonwealth information and enables the prosecution of people who commit those offences.

Defence Act 1903 and Public Service Act 1999 (Commonwealth)

The Defence Act 1903 establishes the structure of the Australian Defence Force and contains similar provisions to the Crimes Act, but is primarily applicable to military Defence members.

The Public Service Act 1999 (Commonwealth) covers disclosure of official information by an Australian Public Service employee.

Freedom of Information Act 1982

The Freedom of Information Act 1982 provides members of the public with the right to access official information held by Defence.

Defence is obligated to meet these requests; except where the disclosure of information could result in harm to the Government, the nation or individuals.

Privacy Act 1988

The Privacy Act 1988 protects an individual's personal information and imposes obligations on Defence and Defence employees to protect any personal information collected.

Defence Force Discipline Act 1982

Australian Defence Force members are required to conform to the rules, laws and obligations defined by the Defence Force Discipline Act 1982. These rules address various forms of criminal conduct; both of a civil and military nature. They also relate to areas such as non-medical use of drugs and consumption of alcohol.

Intelligence Services Act 2001

This Act outlines the functions of the Australian Signals Directorate and the Australian Geospatial-Intelligence Organisation, and the limitations on the activities undertaken by these agencies.

The Act also includes offences for the unauthorised communication, retention and handling of Australian Signals Directorate, Australian Geospatial-Intelligence Organisation and Defence Intelligence Organisation information.

Archives Act 1983

This Act sets out the obligations of Government agencies with regards the treatment, preservation and destruction of official information.

Public Governance, Performance and Accountability Act 2013

This Act sets out the governance, performance and accountability of, and the use and management of public resources by Government agencies.

The Act represents a cultural change in resource management from a compliance approach to a principles-based framework. The Act is based on various principles including the need to 'engage with risk to improve performance'.

Espionage and Foreign Interference Act 2018

This Act modernises and strengthens a range of espionage offences and introduces a number of new foreign interference laws, as well as a new aggravated offence for providing false or misleading information during a security clearance process.

The Act provides Australian law enforcement and security agencies the necessary powers to investigate and the option to pursue prosecution. Criminal charges and imprisonment are now possible consequences for actions that would previously been considered security incidents or breaches of administrative policy.

Defence Security Regime: policy

The Defence Security Regime also consists of policy that outlines your responsibilities as a Defence employee. The key pieces of policy are detailed below.

Protective Security Policy Framework

The Protective Security Policy Framework is a whole of government policy that ensures there is a consistent application of security measures across all Government areas.

Information Security Manual

Designed to complement the Protective Security Policy Framework, the Information Security Manual (ISM) is the whole of government policy standard, governing the security of government ICT systems.

The Information Security Manual is divided into three documents:

1. The Executive Companion provides strategic information on common modes of attack.
2. The Principles Document explains the important concepts and basic principles needed to secure information systems.
3. The Controls Manual contains the detailed controls that technical staff can implement to gain and maintain accreditation.

Defence Security Principles Framework

The Defence Security Principles Framework (DSPF) provides the security policy framework for Defence, by outlining governance, principles and controls applicable to the Defence environment.

The DSPF is primarily designed for Commanders and Managers to enable them to make risk-based decisions for their respective business areas.

Security Standing Orders

Security Standing Orders are the authoritative source documents for localised protective security policy.

Security Standing Orders outline procedures for military and business units, and Defence Industry Security Program members. Security Standing Orders complement and contextualise the Defence Security Principles Framework for the local environment.

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 physical barriers that complement 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.

Measures to achieve Security-in-Depth

Security-in-Depth measures include:

- applying the need-to-know principle

- using a security classification system
- psychological barriers designed to deter intruders
- security alarm systems designed to detect intruders
- physical barriers designed to delay intruders
- security guards trained to respond to alarms
- access control systems to limit access to authorised personnel
- information and communication technology (ICT) security measures designed to protect information technology systems
- Security awareness and training programs.

Forming protective security

Security-in-Depth is achieved through combining a range of protective security measures. These include personnel, physical, information, ICT security, and personal security measures.

Personnel security

Personnel security measures ensure that only people who are deemed suitable and have a genuine need to access official information and material are able to do so. Personnel Security measures also include the maintenance of suitability through an effective 'aftercare' regime.

Physical security

Physical security measures provide a safe and secure environment to protect employees and visitors, prevent unauthorised access to official resources, and deter, detect and delay intruders.

Information security

Information security measures protect official information from unauthorised access or modification, whether in storage, transit or processing.

Information and communication technology security

Information and communication technology security measures protect information stored or transmitted in electronic format.

Personal security

The lines between our professional and personal lives are blurring. Your security responsibilities shouldn't end when you leave the office. Protecting yourself and your family at home is also an important attribute of protective security.

Security specialists

While security is everyone's responsibility, Defence has a network of professional and experienced security specialists who can be called upon for advice and assistance. These are detailed below:

Chief Security Officer (First Assistant Secretary Security and Vetting Service)

The Chief Security Officer (CSO), represented by the First Assistant Secretary Security and Vetting Service, is responsible for directing all areas of the Defence enterprise's security to protect Defence's people, information (including ICT) and assets. The CSO appoints security advisers and ensures staff and contractors are provided information and training to foster a positive security culture. DS&VS responsibilities, on behalf of the CSO, include:

- Security intelligence (such as Security Threat Assessments)
- Developing security policy
- Managing security incidents
- Promoting security awareness
- Training security officers.

Executive Security Adviser

The Executive Security Adviser (ESA) will:

- Support their senior management, Control Owners and Defence Security Committee (DSC) representatives to analyse their security environment and counter unacceptable risks;
- Act as their Group or Service point of contact for security matters;
- Support their Group or Service in maintaining effective Security Officer structures; and
- Provide advice to their Group and Service Security Officer, Control Implementers and Control Officers.

Communications Intelligence Security Officer

The Communications Intelligence Security Officer (COMSO) is the security link within an organisation for the protection of communications intelligence material. A Communications Intelligence Security Officer's responsibilities may include:

- Secure management of CODEWORD material and CODEWORD briefed personnel
- Key roles across protective, personnel, information and physical security.

Security Officer

Every business and military unit has its own Security Officer (SO). Security Officers are the first point of contact for all staff for day-to-day security matters. They are responsible for providing accurate and timely protective security advice to their respective Commanders and Managers.

Security Officers are also responsible for the coordination and administration of the protective security function within their units, including:

- Developing and maintaining Security Standing Orders and security registers
- Conducting briefings - such as induction, travel and departure
- Conducting security compliance checks.

You!

Even if you don't work in a security-based role, you play an important part in Defence's security landscape.

Did you know that 40% of security incident reports relate to lost or stolen Defence passes? This may mean people can gain unauthorised access to Defence establishments. You can help maintain strong security, and foster a good security culture, by protecting your Defence pass and assets.

By being vigilant in your day-to-day activities and reporting things that are out of the ordinary, you can ensure that you play your part in the Defence security landscape.

Module 2: Overview of security threats

At the end of this module, you will be able to:

- identify the SAFEBASE levels
- identify the common threats to security in Defence
- identify how to report security incidents and suspicious contacts.

SAFEBASE - Security Alert Level System

SAFEBASE Security Alert system is a risk management and response tool designed to help protect people and assets on Defence premises from the threat of a violent act. The three levels are detailed below:

AWARE Level

What you need to know:

Threat advice indicates a general warning that Defence could be the target of a violent act, however Defence does not have information about a specific time or location. Normal business is expected. You should know your security responsibilities. Practice your 8 Security Essentials.

How should you behave?

- Be familiar with local security instructions and security measures in your workplace - every Defence establishment is different
- Know who your Security Officer is and where to get security help
- Report security concerns and incidents
- Understand your security environment and where to find information

Timeframe:

Can be maintained indefinitely. Reviewed at least annually.

ALERT Level

What you need to know:

Defence has information that a violent act could happen at your location, within a specific period of time. Expect increased security measures that could delay or restrict your regular duties.

You should consider steps to enhance your personal security and the security of your area.

How should you behave?

- Seek information and advice from your chain of command
- Review security instructions for your work area and focus on actions that you need to take in the event of an incident
- Take part in exercises organised by your SADFO/chain of command
- Be mindful of additional security controls that may impact on day-to-day activities (eg. The SADFO may close an access point or carpark)
- Consider the potential implications to pre-planned events, exercises or meetings (eg. Consider postponing an exercise held on a base or you might move a meeting to another Defence establishment)
- Keep an eye on the establishment's communication channels (eg email) for new instructions or updates
- Report security concerns and incidents

Timeframe:

Maintained for a limited and defined period. To be reviewed at least weekly or as directed by the Chief Security Officer.

ACT Level

What you need to know:

An act is either imminent or happening on your establishment. You should exercise extreme caution and follow emergency procedures.

How should you behave?

- Follow civilian police instructions (eg Australian Federal Police or state/territory police)
- Follow emergency procedures (eg evacuations or lockdown routines) and instructions from your wardens, security authorities, SADFO or Chain of Command
- Take care to avoid putting yourself or others in harm's way
- Stop 'normal' work and, if it is safe to do so, secure classified information
- Report security concerns and incidents, but only when it is safe to do so
- If not inside the establishment, avoid the area.

Timeframe:

Maintained as long as the violent act is underway or expected to be imminent. To be reviewed every 48 hours.

Raising and Lowering Alert Levels

The Chief Security Officer (CSO) is authorised to raise and lower the SAFEBASE levels, nationally, regionally or locally; informed by threat advice and risk assessments.

Senior ADF Officers (SADFO) are authorised to raise or lower SAFEBASE levels locally; informed by threat advice and risk assessments.

Threat actors

Defence has protective security measures in place to protect its people, property, information and activities from threats and sources of harm that could compromise or destroy them. Those seeking to cause harm to Defence are referred to as threat actors.

The most common threat actors that can cause harm to Defence are as follows:

Insider threat

The insider threat involves current or former Defence employees who have, or had, legitimate access to Defence 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.

They may accidentally or intentionally disclose sensitive or classified information, engage in adverse activity such as physical and cyber sabotage, or even harm other employees.

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.

Terrorism

Individuals or groups may use violence, or the threat of violence, against Defence personnel and property to intimidate the Government and the public in order to advance their political, religious or ideological cause.

Criminal groups

Defence 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.

Issue-motivated groups

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 Defence in carrying out its functions.

Defence recognises that Australians have a legal and legitimate right to protest. Defence is only concerned about protests that are likely to be violent or disruptive.

Maverick individuals

A maverick individual is an issue-motivated person, possibly a disgruntled ex-employee, who sees value in causing disruption.

Maverick individuals are generally non-conformists, and may be driven by a particular concern or dispute.

They can sometimes be unstable to deal with, act on impulse and may make poor decisions.

What is the insider threat?

The insider threat may compromise security intentionally to cause harm to Defence (for example, a disgruntled employee), or inadvertently through poor security practices. Insider threat activity can be classified as being either deliberate or unintentional.

Deliberate insider threat

No matter what the individual's motivation, their activity can be harmful, expensive, embarrassing and disruptive. Their actions can also have long-term detrimental effects on Defence's operations, reputation and culture.

Threat actors may use the disgruntled or vulnerable individual to:

- Gain access to Defence information, weapons etc
- Engage in criminal activity including possession, use of and dealing in illicit drugs;
- Engage in physical or electronic sabotage;
- Facilitate third party access;
- Commit fraud, espionage and other behaviours that can harm Defence and its interests.

Unintentional insider threat

Most insider threat activity is unintentional. For example official information can be accidentally disclosed when personnel:

- Do not follow security policy and procedures properly
- Become unmotivated through lack of concern.

Since the proliferation of social media, Defence has seen an increase in unauthorised disclosure of official information through this medium.

This continues to be of security concern.

Suspicious contacts and how to identify them

A contact of security concern, also called a suspicious contact, may occur when a Defence employee is approached by, or communicates with, any individual whose purpose appears to be to obtain official information.

A suspicious contact could involve:

- Social or official interactions
- Verbal or written communication (including the Internet)
- Contacts made in Australia or overseas
- Defence members being followed.

You play an important part when it comes to incident and suspicious-contact reporting.

By remaining vigilant and security aware, you can help to counter threats Defence may face, especially the insider threat.

Defence members should report any contact with an individual of possible security concern that aligns with the acronym SOUP. SOUP stands for **S**uspicious, **O**ngoing, **U**nusual, **P**ersistent or uninvited.

For further information on suspicious contacts and how to report them, refer to the DSPF Principle on Contact Reporting or talk to your Security Officer.

Reporting a suspicious contact

You must report a suspicious contact to your Security Officer and Defence Security and Vetting Service Counterintelligence as soon as possible to allow prompt assessment and appropriate action.

If you think you have been involved in a suspicious contact, you need to contact your Security Officer and complete an XP168 Report of Contact of Security Concern, available online from the Defence Security and Vetting Service Intranet Security Portal and on the Defence Online Services Domain Security Portal.

If you think a colleague has been the subject of a suspicious contact and it has not been reported, then you should report it to your Security Office immediately, and complete an XP168. Third party reports are treated in the strictest confidence.

Personnel working in the Defence Intelligence Agencies are required to submit all security-related reporting through Defence Intelligence Security. For further information, visit the Defence Intelligence Security website.

For further information on suspicious contacts and how to report them, refer to DSPF Principle - Contact Reporting or talk to your Security Officer.

Security incidents

Identifying a security incident

A security incident is any event that prejudices security or breaches security regulations. Such events are often the result of a failure to comply with security policy and can be accidental, negligent or deliberate.

A security incident could include:

- Unauthorised access to Defence establishments or facilities
- Unauthorised use of or attacks on Defence information and communications equipment
- Inappropriate handling or storage of official information
- Accessing information or disclosing it to people who do not have a genuine need-to-know
- Loss, theft or unauthorised access to classified or official information
- Incidents involving weapons, explosive ordnance and/or controlled items
- Any civil police investigation that involves Defence personnel or property
- Acts of espionage, sabotage, or insider threat activities.

Reporting a security incident

You must report all security incidents to your Security Officer and the Defence Security and Vetting Service Security Incident Centre as soon as possible to allow prompt assessment and appropriate action.

If you think you have been involved in a security incident, you need to contact your Security Officer and complete an XP188 Security Incident Report available online.

For further information on security incidents, see the DSPF Principle on Security Incidents and Investigations or talk to your Security Officer.

Module 3: Information security

At the end of this module, you will be able to:

- describe the current system of protective markings
- explain the need-to-hold and need-to-know principles
- understand best practice security and how it applies to handling official information.

Information security

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

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

- documents and papers
- data
- the software or systems and networks on which the information is stored, processed or communicated
- the intellectual information (knowledge) acquired by individuals
- physical items from which information regarding design, components or use could be derived.

You can get further information about Information Security from the DSPF Principle on Classification and Protection of Official Information, by reading your unit's Security Standing Orders, or by talking to your Security Officer.

Protective markings

All information that you handle in an official capacity is defined as official information and must be protected accordingly.

Official information is protectively marked according to the consequences of unauthorised disclosure or compromise of national security and the national interest.

Marking official information allows appropriate security measures to be applied. Depending on the marking, those measures will differ about how the information is to be labelled, stored, moved and destroyed, as well as who can view the information.

Note: Although all information must go through the protective marking process, not all information will be given a security classification.

Protective Markings are covered in depth in Document Handling training.

Best practice for information security

Applying protective markings is only one attribute of information security. There are three other key policies and principles to be adhered to in handling Defence information. These are the need-to-know principle, the need-to-hold principle, and the clear desk and screen policy.

Need-to-know principle

The need-to-know principle says that you must limit official information only to those who need it to do their work.

The need-to-know principle says that having the appropriate security clearance to access the information is only half of the issue. The other half is about limiting official information to those who need it to do their work. Access to official information is not afforded to you solely by virtue of your office, position or security clearance.

Limiting access to official information

Access to official information is not afforded to you solely by virtue of your office, position, or security clearance.

When it comes to need-to-know, it is your responsibility (as the holder of the information) to verify the need-to-know of anyone you share the information with.

This can be hard, as it goes against our natural instincts and everything we have been taught about getting along in groups.

Defence's expectations

1. Limit your requests for information to that which you have a genuine need-to know. Be aware that you may be expected to explain why you need to know it.

2. Refrain from discussing official information where the discussion may be overheard by persons who do not have a need-to-know.

3. If someone asks you for official information, you are expected to ensure they are cleared appropriately and have a genuine need-to-know before you provide any information to them. You are also obliged to report to your Security Officer any co-worker who violates the need-to-know principle.

Need-to-hold principle

The need-to-hold principle is that information should only be retained when it is necessary for the actual performance of duties.

Information should only be retained when it is necessary for the actual performance of duties. Information should be disposed of (archived/destroyed) when no longer required, in accordance with the Archives Act 1983.

Excess physical holdings of information increase:

- The risk of compromise of national security
- The storage and handling costs through the use of excessive physical security controls
- The procedural and monetary cost of recovery, remediation and investigation.

Before you hit print, think about the implications of the material you're printing - consider if there's a genuine requirement to create a hard copy of your information.

Clear desk and screen policy

Ensure that official information is not left unattended and is secured appropriately.

You are responsible for the security of official information under your control.

When absent from the workplace, Defence personnel and external service providers must ensure that official information is not left unattended and is secured appropriately.

This is known as the clear desk and screen policy. If your desk and screen are clear, you are reducing the chance of a security incident occurring.

You can get further information from the DSPF Principle on Classification and Protection of Official Information, or by talking to your Security Officer.

Audio security requirements

Classified information also needs to be protected when communicated in person, by phone or using video conferencing.

Open-plan offices and unsecured environments present an increased security risk due to the ability to overhear conversations. You are not only personally responsible for keeping noise to a minimum within the workplace, but also to be actively aware of your conversations.

Conversations that contain classified material must be conducted in an audio-secure area. An audio-security level is used to describe the audio-security of a room or area.

The DSPF contains the Principles and Controls related to holding classified conversations.

For further information on audio security and video conferencing, see DSPF Principle on Audiovisual Security, or talk to your Security Officer.

Storage of official information

Strict procedures need to be followed when storing official information. The higher the classification, the more elaborate the measures are to ensure security is maintained.

It is essential that you know what the procedures are and how to apply them correctly before you access official information.

Storage requirements for official information are based on three variables:

1. the security of the area where the material is to be stored
2. the level of protection provided by the container
3. the classification or Business Impact Level of the material.

Close of business checks

Each day before you leave, you should check your workspace to ensure it is secure. Think of close-of-business checks in the same light as when you leave your place of residence for a period of time. You wouldn't leave your house and possessions unsecured, would you?

It is recommended that you devise a workplace lock-up procedure like the following:

1. Logging off all systems and switching the screen off.
2. Securing all classified documents and ensuring there is no official information left out in the workplace.
3. Ensuring that laptops and other electronic media storing security official information are secured.
4. Ensuring that there is no classified information in wastepaper bins.
5. Ensuring that whiteboards and other displays do not show any classified information (special care needs to be taken with electronic whiteboards).
6. Ensuring that vaults and containers are locked and that combination locks are spun five times.
7. Ensuring that windows and doors are locked.
8. Ensuring that keys to containers are secured.

Module 4: Personnel security

At the end of this module, you will be able to:

- understand the importance of personnel security
- list a range of changes in personal circumstances which need to be reported
- explain the process for reporting overseas travel.

Personnel security

Personnel Security ensures that access to official information and security-protected assets are limited to personnel who:

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

The underpinning principles of personnel security include:

- determining the appropriate need and level of security clearance for all Defence staff and contractors. This is typically done by Commanders and Managers.
- conducting initial and ongoing reviews of an individual's suitability to hold a security clearance
- continuous workplace monitoring
- security investigations
- security awareness and training.

Security vetting and clearances

The Australian Government Security Vetting Agency is responsible for granting, revalidating and re-appraising security clearances on behalf of most Australian Government agencies and some State and Territory agencies.

An applicant is assessed for suitability against factor areas identified in the Protective Security Policy Framework (PSPF) Personnel Security Guidelines. A decision is then made on whether the applicant is suitable to hold a security clearance and to be granted access to official information.

There are four levels of Personnel security clearance. These are discussed below.

Baseline

A Baseline security clearance permits ongoing access up to PROTECTED information and assets. This is the minimum clearance for Defence personnel and external service providers.

Negative Vetting Level 1

A Negative Vetting Level 1 security clearance permits ongoing access to PROTECTED, CONFIDENTIAL and SECRET information and assets.

Negative Vetting Level 2

A Negative Vetting Level 2 security clearance permits ongoing access to PROTECTED, CONFIDENTIAL, SECRET and TOP SECRET information and assets.

Positive Vetting

A Positive Vetting security clearance permits access to resources at all classification levels, including certain types of caveat and codeword information.

If you have any queries about security clearances, please ring the Australian Government Security Vetting Agency Client Service Centre on 1800 640 450 or refer to the Australian Government Security Vetting Agency website at www.defence.gov.au/agsva.

Reporting changes in personal circumstances

Once granted a security clearance, Defence and defence industry personnel must inform the Australian Government Security Vetting Agency (AGSVA) of any changes to their personal circumstances that may have an impact on their ability to hold a clearance. Changes may include, but are not limited to:

- change in relationship status;
- criminal charges, warnings or convictions;
- any activity that significantly affects your financial situation;
- any event that significantly affects your personal life or physical well being;
- contacts with foreign nationals where they are enduring or of substance;
- contact with foreign intelligence officials or people you suspect might be foreign intelligence officials;
- membership of associations; and/or
- significant change in religious or political beliefs.

Why should I report changes?

Some significant changes in personal circumstances may have the potential to create vulnerability. The vulnerability could be used by foreign governments, issue-motivated groups, criminal elements or others to entice you into providing information or assets belonging to Defence. Commercial organisations may also use changes in your circumstances to gain information that would give them an unfair advantage in dealing with Defence. Some changes could create the perfect environment for insider threat activity.

When Defence and the Australian Government Security Vetting Agency are aware of changes in your personal circumstances, it is less likely that the changes can be used as a lever against you.

Who can report a change?

Anyone can.

You are obliged to report changes in your personal circumstances.

Security Officers and supervisors are to report any changes that they become aware of. If they are unsure whether the person has notified Australian Government Security Vetting Agency of the change, they can also log a report themselves.

If you become aware of changes in your colleagues circumstances that you believe may impact Defence, you are obliged to report it.

How to report changes in personal circumstances

Change of circumstances can be reported via the two forms detailed below:

SVA003 - Change of Circumstances Notification

This form is available on the Australian Government Security Vetting Agency website, and is to be completed by a clearance holder whose personal circumstances have changed.

SVA004 - Change of Circumstances Report

This form is available on the Australian Government Security Vetting Agency website, and is completed by the supervisor, Commander, Manager or Security Officer.

Staff can also provide advice on changes in personal circumstances to the Australian Government Security Vetting by email on the following email address: SecurityClearances@defence.gov.au

Personnel working in the Defence Intelligence Agencies are required to submit all security-related reporting through Defence Intelligence Security. For further information, visit the Defence Intelligence Security website.

Overseas travel requirements

On the topic of reporting, it is important for you to document your overseas travel properly. When travelling overseas, you will need to complete the following steps.

Before you leave

Before you leave on your trip, you need to:

1. Complete an AB644 Overseas Travel Briefing and Debriefing form, as well as arrange a brief from your Security Officer on issues that may be relevant to your trip, as soon as travel dates are known (and, if advised, conforming to timelines in local Security Standing Orders).
2. Obtain travel advice for the countries to be visited or travelled through from the Department of Foreign Affairs and Trade travel advisory website at www.smartraveller.gov.au. Smartraveller is an excellent resource that Defence encourages you to use and register your travel plans on. Department of Foreign Affairs and Trade will have the latest information concerning the

countries you intend to visit. If you do not register with Smartraveller, the Department of Foreign Affairs and Trade may not know who and where you are in case of an emergency situation; and therefore cannot render assistance.

When you return

On your return you should notify your Security Officer, complete the AB644 Overseas Travel Briefing and Debriefing form and then arrange a debrief from your Security Officer to discuss the events that took place during your visit.

Module 5: Physical security

At the end of this module, you will be able to:

- identify some of the physical security controls utilised by Defence
- describe the importance of access controls
- explain your responsibilities relating to your Defence pass.

Physical security

Physical security refers to controls such as physical barriers, access control systems, alarm systems, and security controls used to protect official information, assets and most importantly – our people.

They are implemented at Defence establishments to:

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

Access controls

Effective access control to a base or facility is one of many protective security layers in a Security-in-Depth system. Different access control measures include, but are not limited to:

- Defence access cards
- visitor access passes and escort procedures
- electronic access control systems
- guarding and security attendants
- security inspections and searches.

Physical controls are applied with the intent of preventing unauthorised access and, should a breach occur, providing early detection of unauthorised access, enabling quick response.

Ideally interception should occur before access to the asset, but this depends on the asset and the security objectives. Every Defence employee and member must be aware of their responsibility to be vigilant with respect to any unauthorised access to their area.

Physical security zones

Physical Security Zone methodology is a multi-layered system in which physical security and access control measures combine to provide protection to aggregated information and assets which require more than normal fire and theft protection (security-protected assets).

Physical security zones are not restricted to just buildings. They can be equally applied to large bases and facilities in which security-protected assets are stored and handled. The table below indicates the zones and examples of the areas they may be applied to.

Zone	Short description	Example
1	Unsecured areas and public access.	
2	Low security area; restricted public access, unrestricted Defence personnel and contractor access.	Defence office complexes within initial security boundaries.
3	Moderate security area; limited Defence personnel and contractor access; escorted visitors only.	Defence establishments/bases, internal security rated areas.
4	High security area; strictly controlled Defence personnel and contractor access; escorted visitor access only.	Defence operation and communication centres.
5	Highest security area; strictly controlled Defence personnel and contractor access; escorted visitor access only.	Australian intelligence establishments.

Defence Common Access Cards

Defence access passes are an important part of access control and are provided for a wide range of applications. Defence passes come in a variety of colours, reflecting their application and access levels. These include:

- Australian Public Service staff passes, which are typically blue in colour.
- Australian Defence Force member passes, which are typically purple in colour.
- National Contractor passes, which are typically yellow in colour.
- Visitor passes. These passes are issued and returned daily and are white with a red V to indicate visitor status.
- Base Access Only passes, which are typically red in colour.

Note that many of these passes have multiple applications. For further details of what each pass allows, please visit the National Pass Office Management website, or talk to your Security Officer.

Your pass responsibilities

Your Defence Access Card (commonly referred to as 'your pass') is a key that gives you access to Defence property, assets and information. It is therefore critical that you protect your pass from unauthorised use. Here are some fundamental guidelines to protect your pass:

- secure your pass when you are not wearing it to protect it from loss, theft, damage or unauthorised use
- immediately report a lost pass to your Security Officer and Pass Office
- clearly display your pass for inspection when entering a Defence establishment
- show your pass on demand to security or any appropriate authority
- take your pass off and do not display it when outside Defence establishments
- do not copy, scan or duplicate your pass
- do not lend your pass to another person
- return your pass to the issuing authority when no longer required (for example, when you leave your position or at the conclusion of your contract with Defence).

What happens if I lose my pass?

A lost pass provides an opportunity for Defence's physical security measures to be breached. As soon as you become aware that you have lost your pass, you must report it. Do not wait for it to 'turn up.' Report it immediately.

What happens if I don't wear my pass?

You could be challenged to provide your pass. If you can't produce your pass, Security personnel will be notified immediately and you will be denied entry to the premises.

Note: You should challenge anyone whose pass you cannot visibly see.

What happens when people leave Defence?

Upon resigning/retiring from your area, you are obliged to return your pass.

If you are a supervisor, ensure that personnel resigning/retiring from your area return their pass and are escorted out of the area. You must then return the pass to the nearest Pass Office.

The Pass Office will destroy the card and invalidate access for the individual.

Visitors

If you have visitors at any Defence premises, you are responsible for their access and their behaviour. You are also personally responsible for escorting them at all times and for ensuring they comply with directions from authorised personnel.

During their visit

During the visit you must ensure that your visitor:

- clearly displays their visitor pass
- is supervised at all times
- does not get unauthorised access to official information.

At the end of their visit

At the end of the visit, you must ensure your visitor:

- returns their visitor pass
- leaves the establishment.

Security keys

Security keys are keys that:

- allow access to official information and security-protected assets
- provide access to Security Construction Equipment Committee approved security containers
- are determined by Commanders, Managers or Security Officers.

The effectiveness of a key control system is critical to overall security.

Security measures for keys

The following security measures must be applied by individuals to control security keys:

- Never leave keys unattended
- Keys must be given the same degree of protection as that provided to the highest level of information the key protects
- Keys must only be handled by people with authorisation to access the information they protect A register must be maintained for all keys
- When not required, return keys immediately to your Security Officer, or to the security container/key cabinet, where they are normally stored
- Additional keys must not be cut without proper approval.

Combination locks

Combination locks can also be used to ensure only users with a need-to-know can access information and equipment stored in a particular area.

The combination lock for a security container may:

- be shared with people who have a need-to-know
- not be written down by users - it should be memorised for everyday use.

Security Officers are responsible for making sure that combinations are changed regularly by respective custodians, and for securely storing the written record of all combination lock settings.

Module 6: Information and communication technology security

At the end of this module you will:

- understand the importance of passwords
- understand, recognise and respond to cyber threats
- be able to apply cyber security principles to social media and computer use.

Information and communication technology security

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

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

Personal ICT usage

Defence allows you to have reasonable use of the telephone, email and internet services for personal purposes, subject to technical, operational and security considerations. This use must not affect national security, undermine business continuity and efficiency, or damage the Department's reputation.

Your continued access is dependent on your ongoing compliance with Defence policy.

What do I need to do?

Read and comply with the following policy documents:

- ICT Manual Chapter 3 – Use of Defence ICT Resources
- Defence Communications Manual Chapter 3 – Digital and Social Media.

Passwords

Passwords have become a common part of the security landscape, both in private and professional settings. Your password is like a key; it will grant you access to resources and systems within Defence.

A compromised password may result in unauthorised access to your email and to your system privileges, which may be used against you and against Defence.

Something to think about

Imagine someone accessing your email without your knowledge and then 'effectively' sending emails on your behalf; how could you prove it wasn't you?

Like all keys, passwords are most effective when they are protected and aren't shared or left out in the open.

Never divulge your password to any other person. Any approach for disclosure of your password must be reported to your Security Officer and the Defence Security and Vetting Service.

Locking your workstation

You are personally responsible for all activities that are carried out under your logon. Therefore, if you leave your workstation, you must lock your computer. Remember, it is also a security breach for you to use someone else's computer that has been left unlocked.

You can lock your computer by pressing CTRL+ALT+DEL keys or by pressing Windows and L keys simultaneously.

You unlock your computer by pressing CTRL+ALT+DEL keys simultaneously then entering your username and password.

Unauthorised connections

Consider the following question. Is it okay to charge a phone or device via the USBs on your Defence computer? The answer is no. Even if you are only intending to charge your device, do not plug it into the computer. Any device connected by USB to a Defence machine automatically becomes part of the Defence network and opens up the potential for viruses and malware.

- Do not connect any unauthorised or non-approved devices (including non-Defence thumb drives) to Defence ICT systems.
- Do not charge mobile phones via a Defence computer or ICT system - this includes Defence-issued devices.

Defence personnel must not connect any devices or cables to the Defence ICT systems without proper authorisation and written approval from the appropriate ICT Security Authority.

Portable electronic devices

Portable electronic devices are an ever-present part of our working and private lives. They present unique security challenges due to the:

- rapidly evolving nature
- ability to record and store large amounts of information in almost any conceivable format

- ability to provide a means to exchange that information via fixed and ad hoc networks.

Portable electronic devices include (but are not limited to): Laptops, Tablets, Blackberries, Smartphones, Smart watches, Cameras, Fitness Trackers, Medically essential devices, eReaders etc.

If you are using your personal devices to access Defence information, for example via DREAMS, your device must be operated in a way that meets the security requirements of the appropriate Defence Security Principles Framework (DSPF) Principles and Controls.

Travelling overseas with a personal electronic device

You should carefully consider information security risks when using an electronic device while overseas.

The compromise of your device could have an impact on Defence, its information and its reputation.

Travelling with personal devices

In most countries there is no expectation of privacy on networks provided by internet cafés, hotels, offices or other public places.

This means any information you access over these networks (including social media and banking) may be collected, stored and exploited.

While your personal device may not have Defence information on it, you should be careful when using your device overseas as your personal information is just as important.

Travelling with a work-issued device

When travelling with a device for work purposes, you must read and comply with Standard Operating Procedures for Defence-issued devices.

You should also:

- be aware of where you access this device, the information contained on it and the risk of that information being compromised.
- Immediately report the loss or theft of any Defence provisioned device in accordance with Defence Security Principles Framework Principle – Security Incidents and Investigations.
- ensure you've visited the Australian Signals Directorate website on travelling overseas with an electronic device.

Cyber security

ICT security is of utmost importance to national security and your own personal security. It is not just a Defence issue.

There are common threats you should be aware of include:

- socially engineered emails and messages such as spam, phishing and spear phishing
- unauthorised connections, for example USB thumb drives

- insider threat, intentional acts such as unauthorised disclosure or unintentional acts such as data spills.

Cybercrime statistics

Cybercrime costs, as reported from the Ponemon Institute 2015 in an article titled the Cost of Cyber Crime Global Study.

In 2015, US companies sampled lost approximately $15 million to cybercrime. This is an increase of 19% from 2014.

In Australia, the same report showed for 2015 that there was an increase of 13% in cost of cybercrime from the 2014 figures.

The average time to constrain a cyberattack was 31 days, with an average cost of $639,462.

Every year the insider threat, denial of service and web-based attacks accounted for 55% of all cybercrime costs.

In the 2015 financial year, on average 1.5 cyberattacks each week were successful. Cyberattacks only need to be successful once; defending against them needs to be successful as often as possible.

Socially engineered emails

Sending socially engineered emails is a common technique used in malicious cyber intrusions targeting Australian Government agencies including Defence. These emails attempt to deceive the person receiving the email to download malicious software by clicking on a link or attachment. A socially engineered email is an email that is designed to look legitimate, while aiming to exploit information from you. They fall into three broad categories, detailed below.

Spam

Spam is the electronic equivalent of junk mail. The term refers to unsolicited bulk, and often unwanted, email, for example adverts for pharmaceutical products.

Phishing

Phishing (pronounced as 'fishing') emails attempt to collect personal or financial information or attempt to infect your machine with malware (malicious software).

They often contain hyperlinks to malicious websites, for example emails pretending to be from legitimate financial institutions.

Spear phishing

Spear phishing emails are highly specialised attacks against a specific target, or small groups, to collect information or gain access to systems, for example crafted emails with specific Defence related themes.

Warning: Do not click on a link or attachment in an email if you do not know the sender.

Identifying Socially engineered emails

While socially-engineered emails can be highly sophisticated, there are ways to differentiate them from legitimate emails. Consider the following questions when you next read your emails:

- Do you really know who is sending you the email?
- Are you expecting an email from them?
- Is the content of the email relevant to your work?
- Does the email ask you to access a website or open an attachment?
- Is the web address relevant to the content of the email?
- Is the email from a personal email address?
- Is the email suspiciously written?
- Have you received the same email twice?

If you're keen to learn more, Cyber Security Awareness is available as an eLearning course on Campus.

Who do I need to do if I have received socially engineered emails?

The Defence Gateway employs capabilities to assist with stopping socially engineered emails from entering Defence's email system, however this is not foolproof.

If you feel that you have received socially engineered emails:

- Do not attempt to contact the sender of the email, either by replying to the email or by other means
- Do not open any attachments or click on any hyperlinks
- Report the email using the appropriate process for the type of email as follows:

Reporting Spam

1. create a new email message
2. attach the Spam email to the new email
3. send it to spam@defence.gov.au where it will be reviewed so remedial action can be taken
4. Once you have sent the malicious email to the appropriate area delete them from your Inbox, Sent Items and your Deleted Items in your mail client (Outlook or other email application).

Reporting Phishing

1. call the DPN Service Desk and report the email, indicating that the DSMS ticket should be sent to “Defence Security Operations Centre”

2. create a new email message with a subject line of the DSMS ticket number provided by the DPN Service desk
3. attach the Phishing/Spear Phishing email and send the new email to defence.soc@defence.gov.au
4. Once you have sent the malicious email to the appropriate area delete them from your Inbox, Sent Items and your Deleted Items in your mail client (Outlook or other email application).

Social media

Social media is used by people across Defence and defence industry to communicate with family, friends, colleagues, social groups, employers and others. When used responsibly and with the correct level of security protections applied, the risk to you, those around you and Defence can be successfully managed.

As a member of Defence, you are free to use social media outside of a work environment. However, as an employee, be aware that you may be targeted through information on social media. Remaining diligent about who can see your information as well as what you make available can significantly decrease your risk of being targeted or becoming a victim.

Make sure you know how to protect yourself online.

Official and Unofficial social media profiles

Official and unofficial social media profiles can be divided into three types:

- Official Defence profiles which are developed and approved by Defence. Official profiles communicate announcements, initiatives or activities that go through the approval and clearance process as laid out in the Defence Communications Manual (DCM).
- Unofficial profiles are not endorsed by Defence. They are often created with imagery to make them look like an official Defence profile, seeking to lure APS and ADF members. Where possible, these accounts are monitored and reported to social media platforms when they attempt to damage Defence's reputation.
- Personal profiles are created by personnel for their personal use and are not to contain official or unapproved Government content.

As a member of the Australian Defence Force (ADF) or Australian Public Service (APS), it is important you understand what you are free and able to post online regarding political commentary and messages.

The Defence Communication Manual (DCM) is applicable to all Defence personnel and the following two chapters relate to Social Media -

- Chapter 2 Media engagement and public comment
- Chapter 3 Digital and social media.

The Australian Public Service Commission (APSC) also provides information for members of the APS on making public comments on social media and advises "A Commonwealth employee must not make public comment that may lead a reasonable person to conclude they cannot serve the government of the day impartially and professionally."

Public comment on Social Media

In 2013, a public servant was sacked for anonymously tweeting her private views about Australia's immigration policies.

More than 9,000 tweets were posted under the Twitter handle LaLegale covering topics from 'our invasion of Iraq' to offshore processing.

An investigation found she had not upheld public service values by not adhering to guidelines on the use of social media, and making public comments even in an unofficial capacity.

Social Media - an intelligence collection tool

Threat 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.

Approaches may look like:

- 'Friend' requests from unknown sources or people
- Unusual posts or comments
- Invites to join a group
- Strange/flattering emails or invites.

What information do threat actors look for on social media?

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

Aggregation of information on social media can add up and reveal more about you and Defence than you intended.

Social Media – a threat to Defence and Defence personnel

In 2015 during Exercise Talisman Sabre, a number of ADF members were found to have posted a range of field imagery and unauthorised Defence material on personal social media accounts.

Posted information included:

- Field exercise video and imagery

- Defence assets
- Potentially inflammatory views and comments
- Personally identifiable information such as passports and Defence passes
- Geotagged images.

In each case, these accounts were found to be open and accessible by all members of the public.

The use and compromise of social media platforms by a range of threat actors to gain sensitive information is continuing to increase significantly as the use of these sites continues to increase.

- In 2012 hackers compromised LinkedIn and stole the emails and passwords of over 6.5 million users.
- In 2012 media published the results of an investigation into more than 200 current and former intelligence officers who disclosed roles and employment on LinkedIn.
- In 2015 an issue motivated group published a database of 27 000 individuals, including Australians, who they believed worked for or were associated with intelligence agencies. Information was sourced from LinkedIn.

Be mindful of what information you post, how many accounts you own and how this might be used by threat actors if it became compromised.

Social Media – security considerations

To help protect yourself when using social media, consider the following details:

Settings and preferences

- Understand how to apply privacy settings and preferences to restrict access to your profiles.
- Ensure terms and conditions related to use of specific social media applications do not conflict with APS or Departmental policies.
- Be aware that privacy settings change over time and you may need to check them periodically to ensure you're still secure.
- Consider disabling any automatic geo-tagging settings on your electronic devices.

Malicious adversaries

- Be aware that social media websites are a common way for malicious adversaries to gain intelligence.
- Carefully consider whether you identify yourself as a Defence member, employee or contractor on public forums and account profiles.
- Do not post images of members in uniform on non-Defence sites.

- Be aware that people online may disguise their real identity.
- Do not join or maintain membership of a group, forum, site or discussion that is involved in or promotes exploitative, objectifying or derogatory behaviour.

Personal Information

- Carefully consider the personal information you disclose, such as age, address and other identifying information.
- Do no tag photos of friends and colleagues without their permission.
- Carefully consider whether to post information or images that may damage personal or professional reputations, either immediately or in the future.

Additional guidance around your social media responsibilities is contained in the Defence Communications Manual. This provides additional steps you can take to safeguard yourself and Defence.

Pattern of life

A pattern of life is reconnaissance of routine - defining the locations that a subject visits and where they are likely to be at a particular time of day. If you are active on social media, you could be revealing more information than you realise.

Before posting information online, consider what the information could reveal about you or your daily activities, in particular if a conversation, image or location suggests:

- work at Defence or a Defence site
- contacts who may be colleagues
- when you're going out and the location
- when you go on holidays and are not likely to be at home
- previously tagged locations, each of which will be time and date stamped, and may give hints about where you live and your daily routine outside work.

Geo-services: Geotags

A geotag is additional data (metadata) that is provided in various media, particularly in videos and photographs. This data may consist of GPS coordinates, though they can also include altitude, bearing, distance, accuracy data, and place names. Whilst this information can be useful, it can also pose security risks.

Before you upload photos and videos, especially to social media, consider what information may be embedded in the background. Ask yourself if any of this information has the potential to compromise your own security or the security of Defence.

See Australian Signals Directorate publications for additional information on protecting against geotagging on your devices.

Geo-services: Geocoding

Sometimes what's in the photo you take is providing just as much information as what is embedded in the backend code. This concept is known as geocoding. Geocoding refers to the process of taking non-coordinate based geographical identifiers, such as a street addresses, uniforms and buildings.

For example, a photograph of a Defence employee taken on their first day in a new job at the front of their workplace, could show more than intended, such as:

- What they physically look like
- Where the new job is, including visual indicators such as a logo and a street address
- An indicator of what they are likely to wear to work - this is particularly relevant if a uniform is involved
- If they are wearing a pass then possibly a photo ID, which may then be used to compromise access.

This information can also be used to piece together movements and location, which may compromise security.

Think before you post; what is in the image, and do others need to see this information.

Top tips to stay secure online

Tip 1: Be aware that anything you post online can be seen by others, even on a secure site. Others can hack in to your online profile and access your information.

Tip 2: Do not post offensive comments or material.

Tip 3: Do not post dates, locations, unit numbers, names, photographs of you in uniform, or details about missions or operations. Much of this information is classified and posting it on unclassified websites is a security violation.

Tip 4: Think twice about posting any personal details including that you work with Defence, your date of birth, home address, phone number or information about your routine. A basic rule to remember is: if it could be used against you or your family in any way, don't post it!

Tip 5: If you have family and friends accessing social networking sites, educate them about what information they should not post or discuss online, and why.

Tip 6: Only accept friend requests from people you know personally and remove any that you don't. Criminals and Foreign Intelligence Services can create fake profiles and try to add you as a friend to gather information.

Tip 7: Do not open or respond to emails from unknown sources.

Tip 8: When installing apps, widgets and games on your devices read the terms and conditions so you know what personal information they have access to from your profile.

Security Awareness Assessment

An accessible version of this assessment is available for staff who require it, which includes suitability for a screen reader. Requirement is subject to the Web Accessibility Guidelines (see Annex A of this document). If you do not have a disability type as outlined by these guidelines, you are required to complete the Security Awareness course through Campus or Campus Anywhere.

To request an accessible copy version of the assessment, please send an email to: DSVS.Skilling@defence.gov.au

In your email, please provide a brief statement outlining your disability so an appropriate assessment can be tailored to suit your training needs. Instructions detailing how to return your assessment will be included.

Your assessment will be marked and results recorded.

Annex A: Extract of Web Accessibility Guidelines

Accessibility - What does it mean?

"It is essential that the Web be accessible to everybody, regardless of their age, ethnicity or disability"

In order to provide equal access and equal opportunity to people with diverse abilities, the UN Convention on the Rights of Persons with Disabilities recognises access to information and communications technologies, including the Web, as a basic human right. The Australian Government requires that websites are available to as many people as possible. The Disability Discrimination Act (1992) states that agencies must ensure that people with disabilities have the same fundamental rights to access information and services as others in the community.

Accessibility means considering these types of disabilities:

- blindness and low vision
- deafness and hearing loss,
- learning disabilities,
- cognitive limitations,
- limited movement,
- speech disabilities,
- photosensitivity; and/or
- a combination of these.

There are many websites to assist with understanding accessibility. These include the following.

W3C Web Accessibility Initiative (WAI). The WAI provides a list of websites that can be used as Accessibility standard resources.

Web Content Accessibility Guidelines (WCAG). The Web Content Accessibility Guidelines (WCAG) documents explain how to make Web content more accessible to people with disabilities. Web "content" generally refers to the information in a Web page or Web application. This includes documents, text, imagery, forms, sounds, links and others.

Vision Australia. Vision Australia provides information and guides on assistive technology for many vision related impairments.

4syllables. The 4syllables website has useful information on how to meet accessibility and has many downloadable references.

Why do I need to know what Accessibility is and how it affects me?

- Defence, as part of whole of Government, has signed up to the Web Accessibility National Transition Strategy (NTS).
- The NTS sets a course for improved web services, paving the way for a more accessible and usable web environment that will more fully engage with, and allow participation from, all people within our society.

The WCAG 2.0 compliance is all about making websites more accessible to people with disabilities. Web "content" generally refers to the information in a Web page or Web application, including text, images, forms, sounds, and such.

How does accessibility effect my web browsing?

Some commonly used browsers require different settings to allow users to make the website more viewable. Pointers on how to make viewing websites more pleasant are found at the Media Access Australia (MAA) website. The MAA website has information and links to other websites that provide methods on altering text size, setting defaults for popular browsers and other tools.