Module 7 - Security

Module Content	LO 7.1 - Contribute to the maintenance of RAN security
Pre-requisite Modules	
Module Classification	UNCLASSIFIED
Related Assessments	SA2 - GSDR Summative Assessment 1 FA12 - Adele online Quiz
Description	On completion of this module recruits will have gained the underpinning knowledge and skills to comply with RAN protective security regulations.
Delivery Method	This module requires face to face theoretical instruction supported by contextualised practical exercises. It is essential that any delivery strategy is generalist by nature and supported by practical demonstration, role plays and Scenario's. All recruits are expected to consolidate the formal in class instructional presentations with self-paced revision and quiz completion within the Adele LMS.
Key Resources	
WHS Requirements	
Additional Comments	

Durations

Phase	Off Job		On Job	
	Hours	Days	Hours	Days
Module 7-Security				
LO 7.1 - Contribute to the maintenance of RAN security	8	1.07		
Total Duration	**8**	**1.07**		
Summative Assessments				
SA2 - GSDR Summative Assessment 1	1	0.13		
Total Duration	**1**	**0.13**		
Formative Assessments				
FA12 - Adele online Quiz	12	1.6		
Total Duration	**12**	**1.6**		
Other Activities				
Total Duration				
Module Total Duration	21	2.8	21	2.8
	EXCLUDING on job		INCLUDING on job	

LO 7.1 - Contribute to the maintenance of RAN security

LO Classification	UNCLASSIFIED
Performance Conditions	
Performance Standard	Effective participation as a member of duty watch, asisting in the maintenance of security of RS and its surrounds. This Module is summatively assessed through the Summative assessment 1, hosted in ADELE or through the successful completion of the CAMPUS Mandatory awareness training assessment.
Assessment Criteria	
Related Assessments	SA2 - GSDR Summative Assessment 1 FA12 - Adele online Quiz
Related VET Competencies (UoC)	
Content Summary	This LO contains the knowledge and skills required to follow the security procedures required for working in a military environment.
Training Level	NA
Delivery Method	This LO will be delivered via formal classroom lessons. This lesson is able to be delivered at sea on the sea training platform. This is due to the non mandatory nature of this module in the early stages of recruit training. However, the module is a mandatory proficiency requirement prior to graduation. For programming purposes there are no reliances on any other module for effective assessment of the module and is suitable for delivery at any stage within the course program. Prior to the commencement of this CLO Recruits are to complete the Cyber Awareness course in CAMPUS. (Campus Code 00008496)
Resources Required	Human Resources: • 1 x RIC qualified instructor Physical resources: • Fully equipped Recruit School Classroom • Recruit School Module book • DSPF website • Training aids (Security classification folders, videos)
References	Defence Security Principles Framework (DSPF) GSDR Workbook Campus Cyber awareness course
Additional Comments	Assessment Method: The outcomes of this module are predominately theory based and will be assessed through observation and the completion of the formative and summative written exam IAW theoretical assessment plan.
On Job Duration	
Off Job Duration	

Durations

Phase	Off Job		On Job	
	Hours	Days	Hours	Days
LO 7.1 - Contribute to the maintenance of RAN security				
SLO 7.1.1 - Maintain protective security	0.5	0.07		
SLO 7.1.2 - Maintain physical security	0.5	0.07		
SLO 7.1.3 - Maintain personnel security	0.5	0.07		
SLO 7.1.4 - Maintain information security	0.5	0.07		
SLO 7.1.5 - Maintain information, communication and technology (ICT) security	0.5	0.07		
SLO 7.1.6 - Conduct security rounds	5.5	0.73		
Total Duration	**8**	**1.07**		
Summative Assessments				
SA2 - GSDR Summative Assessment 1	1	0.13		
Total Duration	**1**	**0.13**		
Formative Assessments				
FA12 - Adele online Quiz	12	1.6		
Total Duration	**12**	**1.6**		
Learning Outcome Total Duration	21	2.8	21	2.8
	EXCLUDING on job		INCLUDING on job	

Where this LO is assessed as part of a holistic assessment, the duration is only displayed in the Section 1 Durations table.

SLO 7.1.1 - Maintain protective security

Performance Conditions	Recruits will be assessed in a classroom environment at Recruit School, HMAS CERBERUS.
Performance Standard	
Assessment Criteria	7.1.1.1 Define national security 7.1.1.2 Identify major threats to national security 7.1.1.3 Define Protective Security 7.1.1.4 Describe the “security in depth” principle
Related Assessments	SA2 - GSDR Summative Assessment 1 FA12 - Adele online Quiz
Delivery Method	This Learning Outcome will be delivered by the class instructor as a formal classroom theoretical lesson.
Resources Required	Human Resources: • 1 x RIC qualified instructor Physical resources: • Fully equipped Recruit School Classroom • Recruit School Module book • Defence Security Manual DI(G) ADMIN 20-29 • Training aids (Security classification folders, videos)
Teaching Points	IAW the LMG
References	
Additional Comments	
On Job Duration	
Off Job Duration	30 Minutes

SLO 7.1.2 - Maintain physical security

Performance Conditions	Recruits will be assessed in a classroom environment at Recruit School, HMAS CERBERUS.
Performance Standard	
Assessment Criteria	7.1.2.1 Define physical security 7.1.2.2 State measures used to maintain physical security 7.1.2.3 State the purpose of the SAFEBASE alert system 7.1.2.4 List close of business routines
Related Assessments	SA2 - GSDR Summative Assessment 1 FA12 - Adele online Quiz
Delivery Method	This Learning Outcome will be delivered by the class instructor as a formal classroom theoretical lesson.
Resources Required	Human Resources: • 1 x RIC qualified instructor Physical resources: • Fully equipped classroom for maximum 24 recruits • Recruit module book • Access to the Intranet and Internet • RSSO-R
Teaching Points	IAW the LMG
References	
Additional Comments	
On Job Duration	
Off Job Duration	30 Minutes

SLO 7.1.3 - Maintain personnel security

Performance Conditions	Recruits will be assessed in a classroom environment at Recruit School, HMAS CERBERUS.
Performance Standard	
Assessment Criteria	7.1.3.1 Define personnel security 7.1.3.2 List measures used to maintain personnel security 7.1.3.3 State an individual's responsibilities to maintain personnel security 7.1.3.4 List exploitable weaknesses in personal character
Related Assessments	SA2 - GSDR Summative Assessment 1 FA12 - Adele online Quiz
Delivery Method	This Learning Outcome will be delivered by the class instructor as a formal classroom theoretical lesson.
Resources Required	Human Resources: • 1 x RIC qualified instructor Physical resources: • Fully equipped Recruit School Classroom • Recruit School Module book • Defence Security Manual DI(G) ADMIN 20-29 • Training aids (Security classification folders, videos)
Teaching Points	IAW the LMG
References	
Additional Comments	
On Job Duration	
Off Job Duration	30 Minutes

SLO 7.1.4 - Maintain information security

Performance Conditions	Recruits will be assessed in a classroom environment at Recruit School, HMAS CERBERUS.
Performance Standard	
Assessment Criteria	7.1.4.1 Define information security 7.1.4.2 Identify the Australian Government Security Classification System markings 7.1.4.3 Identify Dissemination Limiting Markers 7.1.4.4 Describe the principles of need to know and need to hold
Related Assessments	SA2 - GSDR Summative Assessment 1 FA12 - Adele online Quiz
Delivery Method	This Learning Outcome will be delivered by the class instructor as a formal classroom theoretical lesson.
Resources Required	Human Resources: • 1 x RIC qualified instructor Physical resources: • Fully equipped classroom for maximum 24 recruits • Recruit module book • Access to the Intranet and Internet • RSSO-R
Teaching Points	IAW the LMG
References	
Additional Comments	
On Job Duration	
Off Job Duration	30 Minutes

SLO 7.1.5 - Maintain information, communication and technology (ICT) security

Performance Conditions	Recruits will be assessed in a classroom environment at Recruit School, HMAS CERBERUS.
Performance Standard	
Assessment Criteria	7.1.5.1 Define ICT security 7.1.5.2 State measures to maintain ICT security
Related Assessments	SA2 - GSDR Summative Assessment 1 FA12 - Adele online Quiz
Delivery Method	This Learning Outcome will be delivered by the class instructor as a formal classroom theoretical lesson.
Resources Required	Human Resources: • 1 x RIC qualified instructor Physical resources: • Fully equipped classroom for maximum 24 recruits • Recruit module book • Access to the Intranet and Internet • RSSO-R
Teaching Points	IAW the LMG
References	
Additional Comments	**Pre-requisites:** Campus Cyber awareness course
On Job Duration	
Off Job Duration	30 Minutes

SLO 7.1.6 - Conduct security rounds

Performance Conditions	Recruits will be assessed in a classroom environment at HMAS CERBERUS.
Performance Standard	
Assessment Criteria	7.1.6.1 Define the RAN security organisation 7.1.6.2 Describe the role of personnel within the security organisation 7.1.6.3 Identify a security breach 7.1.6.4 Describe the actions to be taken upon discovering a security breach 7.1.6.5 Conduct security rounds IAW relevant SSOs
Related Assessments	SA2 - GSDR Summative Assessment 1
Delivery Method	This Learning Outcome will be delivered by the class instructor as a component of the Duties and responsibilities of Duty Watch personnel. It is one of the duty watch stations and is embedded within the Duty Watch round Robin. Duty Watch Round Robin includes: • Security Rounds • Role of QM and QMA • Colours and sunset, and The round robin is to be conducted as an informal walk around that provides the theoretical reasoning for members of duty watch, while providing the physical and observable skills required of Duty Watch members.
Resources Required	Human Resources: • 1 x RIC qualified instructor Physical resources: • Fully equipped Recruit School Classroom • Recruit School Module book • Defence Security Manual DI(G) ADMIN 20-29 • Training aids (Security classification folders, videos)
Teaching Points	IAW the LMG
References	
Additional Comments	Security rounds are conducted by Recruits as part of Duty Watch rotations. Time allocated on Job represents approximate performance of role while undertaking Duty watch requirements.
On Job Duration	
Off Job Duration	330 Minutes

CAMPUS COURSE TRAINING RECORD

COURSE TITLE	CAMPUS COURSE NUMBER	COMPLETE BY	SIGNED
Hazardous Chemicals Awareness	00042215	End of Week 2	
Defence Youth Safety Awareness L1	00011653	End of Week 2	
Defence Youth Safety Awareness L6 (U/18) or	00012751	End of Week 2	
Defence Youth Safety Awareness L6 (Adults)	00012752	End of Week 2	
COVID-19 ADF Awareness	Via Defence Coronavirus 19 Training Packages on ADELE	End of Week 3	
SeMPRO General Awareness	00014972	End of Week 3	
Indigenous Cultural Awareness	00007208	End of Week 3	
Cyber Security Awareness	00008496	End of Week 3	
Assessing and Protecting Official Information	00074829	End of Week 4	
Fraud and Integrity Awareness	00073439	End of Week 4	
Defence Fatigue Awareness eLearning	00034708	End of Week 4	
Hearing and Noise Awareness	00009711	End of Week 4	
Defence Heat Illness and Injury	00013512	End of Week 9	
Introduction to the Laws of Armed Conflict	00074609	End of Week 9	
Mortuary Affairs Level 1 Awareness	00063155	End of Week 9	
ADELE Military History Module	Via GSDR ADELE	End of Week 9	

All of the above courses must be completed by the dates listed .They are not programmed and are the responsibility of the Recruit to ensure the training is completed. You will need to allow about 40 minutes for each course. Ensure you print out the certificate as evidence of completion and present it with this record to your Instructor for signature.

7.1 Contribute to the Maintenance of RAN security

MODULE LEARNING OUTCOMES AND ASSESSMENT CRITERIA

7.1 Contribute to the Maintenance of RAN security

7.1.1 Maintain Protective Security
- 7.1.1.1 Define National Security
- 7.1.1.2 Identify major threats to National Security
- 7.1.1.3 Define Protective Security
- 7.1.1.4 Describe the “Security in Depth” Principle

7.1.2 Maintain Physical Security
- 7.1.2.1 Define physical security
- 7.1.2.2 State measures used to maintain physical security
- 7.1.2.3 State the purpose of the SAFEBASE alert system
- 7.1.2.4 List close of business routines

7.1.3 Maintain Personnel Security
- 7.1.3.1 Define Personnel Security
- 7.1.3.2 List measures used to maintain Personnel Security
- 7.1.3.3 State an individual’s responsibilities to maintain Personnel Security
- 7.1.3.4 List exploitable weaknesses in personal character

7.1.4 Maintain Information Security
- 7.1.4.1 Define Information Security
- 7.1.4.2 Identify the Australian Government Security Classification System markings
- 7.1.4.3 Identify Dissemination Limiting Markers
- 7.1.4.4 Describe the principles of need to know and need to hold

7.1.5 Maintain Information, Communication and Technology Security
- 7.1.5.1 Define ICT security
- 7.1.5.2 State measures to maintain ICT security

7.1.6 Conduct Security Rounds
- 7.1.6.1 Define the RAN security organisation
- 7.1.6.2 Describe the role of personnel within the security organisation
- 7.1.6.3 Identify a security breach
- 7.1.6.4 Describe the actions to be taken upon discovering a security breach

References:
Defence Security Principles Framework (DSPF)
Protective Security Policy Framework (PSPF)
Information Security Manual (ISM)
Class Standing Orders
Section Security Orders

SECURITY RESPONSIBILITY

“The Australian Government is responsible for the Security of the Nation.”

DEFININITION OF NATIONAL SECURITY

"NATIONAL SECURITY IS THE TERM USED TO DESCRIBE THE SAFETY OF THE NATION FROM _____, SABOTAGE, _____ MOTIVATED VIOLENCE, PROMOTION OF COMMUNAL VIOLENCE, _____ ON AUSTRALIA'S DEFENCE SYSTEM, AND ACTS OF FOREIGN _____."

THE THREAT

While some security threats are found to be intentional (e.g. espionage), most incidents are not. They are actually a result of poor security practices in the workplace. This means each one of us have a significant opportunity to combat security threats on a daily basis.

It is also important to understand that although there are many different types of security threats, there are only five common sources for those threats.

a. **Trusted Insider** - Internal threats come in a variety of forms including the accidental disclosure of sensitive information; disgruntled staff looking to get back at Defence; and staff that are specifically targeted by external threat sources.

b. **Foreign Intelligence Services** - Foreign Intelligence Services want to discover our Defence capabilities.

c. **Terrorism** - People that use or threaten to use violence against individuals or property in an attempt to coerce or intimidate governments, societies or communities to achieve ideological, political or religious objectives.

d. **Issue Motivated Groups** - An issue motivated group can be defined as a collection of activists with a common ideology that engages in political activities but is not a registered political party. However, extreme groups can engage in 'direct action', such as blockading Defence facilities or trespassing into Defence exercise areas even personal assaults.

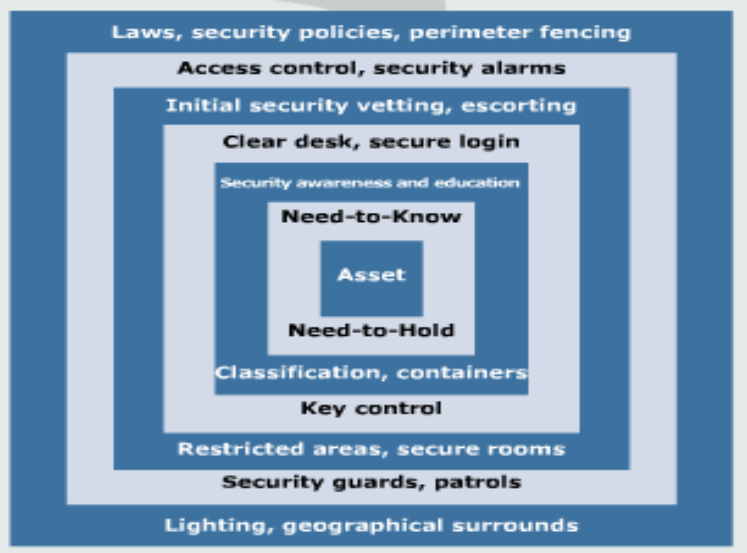
e. **THE BELIEF THAT THERE IS NOT THREAT**.

PROTECTIVE SECURITY

Protective security is the total concept of information, personnel, physical and information & communications technology (ICT).

SECURITY IN DEPTH PRINCIPLE

Defence employs a strategy of security-in-depth to protect its people, information, assets and infrastructure from sources of harm that could weaken compromise or destroy them. Security in depth is achieved through a protective security regime consisting of a combination of physical, personnel, information, and information and communications technology (ICT) security measures.



DEFINE PHYSICAL SECURITY MEASURES

Physical security applications are based on site-specific security risk assessment and the Security -in-Depth principle.

PHYSICAL SECURITY

Physical security applications on a facility or building include:

a. Guard posts;

b. Defence security passes;

c. Perimeter fences and gates;

d. External and internal facility guard patrols;

e. External and internal CCTV systems;

a. Security alarm systems;

f. Other access control measures such as cipher locks and biometric systems;

g. Security Keys; and

a. Security Containers.

PHYSICAL SECURITY DEFINITION

Physical security is broken into the security principle and security rationale.

PHYSICAL SECURITY PRINCIPLE

The security principle defines ‘defence facilities, people, official information, and security protected assets are protected from unauthorised access, sabotage, wilful damage, theft or disruption through a safe and secure physical environment.

PHYSICAL SECURITY RATIONALE

The physical security rationale is the application of physical security measures consistent with whole of government requirements, it will:

- Ensure a secure physical environment for storage and handling of official resources;

- Facilitate sharing of information and assets across government, with allies and persons engaged under contract.

- Maintain a safe and secure working environment for defence personnel and persons engaged under contract.

PHYSICAL SECUIRITY MEASURES

There are several different types of security measures that may be implemented depending on the alert level and level of classification being held on a premise. They generally will be a combination of the below:

- Perimeter fences and gates
- Guard posts / access points
- External and internal facility guard patrols
- External and internal CCTV systems
- Security alarm systems
- Other access control measures such as cipher locks and biometric systems.
- Security Keys
- Security Containers
- SAFEBASE Alert System

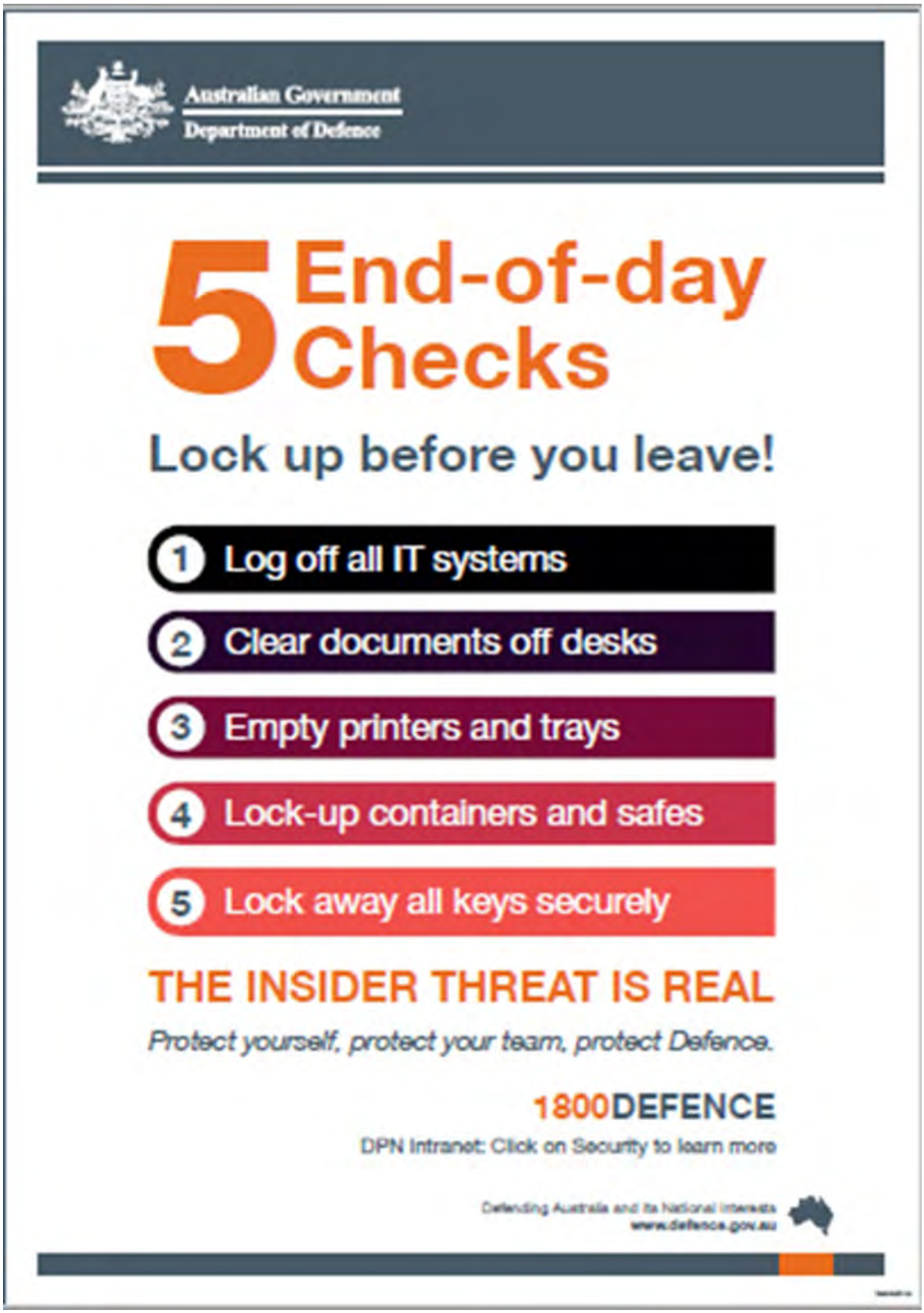
DEFENCE COMMON ACCESS CARDS (DCAC)

When you work at a Defence site you are required to wear a security pass known as a Defence Common Access Card (DCAC) or more commonly referred to as your ID. The DCAC entitles the holder to unescorted access to facilities for which they have the appropriate security clearance, and a legitimate need to access. You must wear the DCAC at all times in the Defence environment and it is your responsibility to:

a. Wear your pass above the waist on Defence premises.

b. Remove your pass from sight when leaving the premises to avoid attracting attention.

Before securing each day, the following checklist is to be followed:



SAFEBASE DEFENCE SECURITY ALERT SYSTEM

Safe Base is Defence's security alert system; it communicates the threat of violent acts on defence premises. It is a risk management and response tool underpinned by effective security planning.

SAFE BASE has three levels of alert dependant on the threat. The levels are:

a. **AWARE:** Security aware - Threat advice indicates a general warning that Defence could be the target of a violent attack. No specific time or location.

b. **ALERT:** Increased security - Threat advice of potential attack or act of violence expected in a specific region or specified Defence site, with a specific timeframe.

c. **ACT:** Follow emergency procedures - Attack on Defence premises is imminent or underway

PERSONNEL SECURITY

Personnel Security is 'The taking of responsible and practical measures to ensure that only _____, _____ and _____ persons who have an established need are permitted access to classified Defence information and assets'.

THE FOUR LEVELS OF PERSONNEL SECURITY CLEARANCES ARE:

BASELINE: Permits access to information or resources up to and including PROTECTED.

NEGATIVE VETTING – LEVEL 1 (NVL1): Permits ongoing access to information or resources up to and including SECRET.

NEGATIVE VETTING – LEVEL 2 (NVL2): Permits ongoing access to information or resources up to and including TOP SECRET. CONFIDENTIAL, SECRET and TOP

TOP SECRET POSITIVE VETTING (TSPV): Permits access to certain types of sensitive, caveated, compartmented and codeword information.

PERSONNEL SECURITY MEASURES

a. Security vetting and clearances;

b. Security education;

c. Control of access/need to know;

d. Monitoring of overseas travel; and

e. Punitive measures for unauthorised disclosure of official information.

CHANGE IN PERSONAL CIRCUMSTANCES

Reporting changes in circumstance helps entities assess personnel security risk based on current and relevant information. Early identification of changes in risk profiles can prevent smaller issues from becoming larger problems. At the individual level, this means encouraging and enabling self-reporting of changes in circumstance by personnel.

EXPLOITABLE WEAKNESSES OF PERSONNEL (PRIMED):

- **P**romiscuity
- **R**evenge
- **I**deology
- **M**oney
- **E**go
- **D**rugs

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.

AUSTRALIAN GOVERNMENT SECURITY CLASSIFICATION SYSTEM (AGSCS)

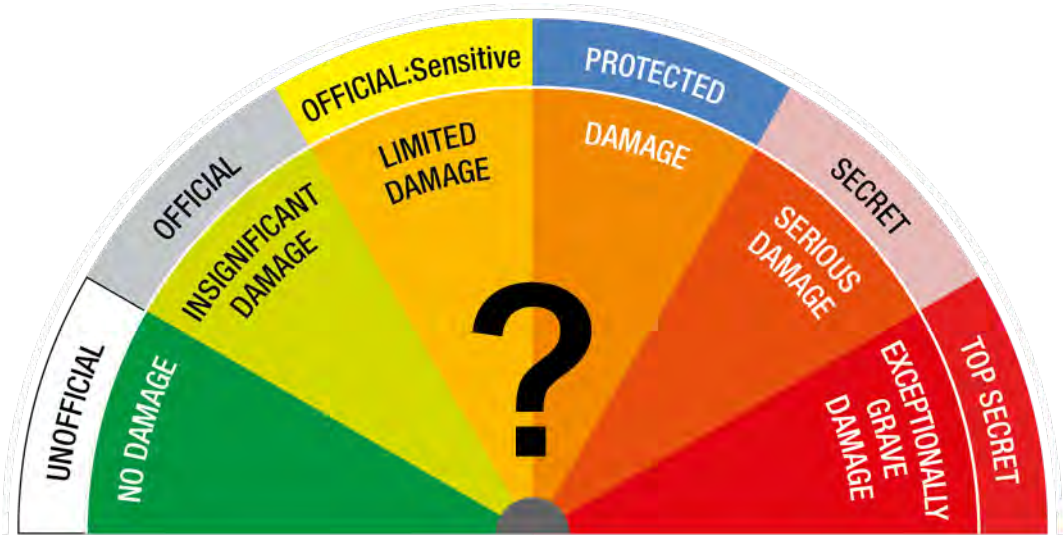
A classification level is used to indicate the relative importance of classified information to national security and thereby determines the specific security requirements applicable to that information. Clearly defined classification levels are essential to an effective classification system.

The **Australian Government Security Classification** system has six levels:

Classification	*Identification Colour*	*Consequence*
Top Secret	Red	Exceptional grave damage
Secret	Salmon	Serious damage
Protected	Blue	Damage
Official: Sensitive	Yellow	Limited damage
Official	Grey	Insignificant damage
Unofficial	White	No damage

ASSESS THE DAMAGE

When handling classified information, think to yourself how much damage would it cause if the information was leaked or made public, what damage could it cause to **people**, **organisations** or **government**?



INFORMATION MANAGEMENT MARKERS (IMM)

An IMM is a marking that is used for information where disclosure may be limited or prohibited by legislation, or where it may otherwise require special handling. There are three categories of IMM:

1. Legal Privilege
2. Legislative Secrecy
3. Personal Privacy

NOTE: IMM'S ARE NOT SECURITY CLASSIFICATIONS.

OFFICIAL INFORMATION

All information related to your work for Defence is **OFFICIAL** information.

Examples may include:

- Hand written notes that you take at a Defence meeting.
- An email to a work colleague about a defence matter.
- Information on a website in the Defence Protected Network.

UNOFFICIAL INFORMATION

Information relating to your social or home life is **UNOFFICIAL** information.

Examples may include:

- An invitation to meet someone at the gym.
- Calling your mechanic about a car service.
- Arranging tennis coaching for the weekend.

NEED TO KNOW

This principle requires that access to classified information that is limited to those who are appropriately cleared and need to use it for their work.

LOOSE OR UNGUARDED TALK

Regardless of how good our classification system or need to know and hold is, it will not be effective if classified information is discussed in inappropriate locations. Always be mindful of where, who and what is around you.

The following are examples of subjects not to be discussed or revealed to persons other than service personnel with a need to know.

a. All classified information;

b. Movements of HMA Ships;

c. Details/Results of operations (exercise), equipment trials;

d. Capabilities and limitations of ships and their equipment;

e. Technical details of weapons and weapon systems;

f. Technical details of military communications and electrical equipment; and

g. Identification of key personnel.

“LOOSE LIPS SINK SHIPS”

NEED TO HOLD

The NEED-TO-HOLD principle requires that classified documents or material are to be held only by those individuals or units who have a need for immediate access to them.

STORAGE, TRANSFER AND DISPOSAL

All classified information has strict procedures for handling. In particular:

a. Storage (containers);

b. Transfer (envelope treatment, seals, registers); and

c. Disposal (shredding, placement within classified waste bag).

INFORMATION COMMUNICATION TECHNOLOGY (ICT)

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

- Computers (including internet and social media)
- Personal Electronic Devices (PEDs)
- Phones
- Multi-Function Devices
- Cyber and Multimedia

Defence has significant measures in place to ensure ICT security depending on the method. These can be:

- Procedures and processes
- Classifying information
- Labelling of devices and information
- Controlling access
- Classified material registers
- Securing ICT equipment and media

When ICT equipment is not in use, it must be secured in an approved container, vault or compartment.

RAN SECURITY ORGANISATION

The RAN security organisation sits underneath the Chief Security Officer who reports to the Chief of Defence Force and Secretary of Defence.

In accordance with the PSPF, the **Chief Security Officer** is responsible for directing all areas of the Defence enterprise's security to protect Defence's people, information and assets.

Defence Policing and Security - Navy	DPS-N	Rank of Captain
Unit Security Officer	USO	LCDR / LEUT
Joint Military Policing Unit	JMPU	Tri Service Policing
ALL PERSONNEL		

RAN SECURITY ORGANISATION DUTIES AND RESPONSIBILITIES

DEFENCE POLICING AND SECURITY - NAVY DPS-N

DSEC-N is responsible for Navy security development and the provision of specialist advice to the CN and sub-program managers consistent with approved Defence policy for Physical, Personnel and Information Systems security.

UNIT SECURITY OFFICER USO

The Unit Security Officer (USO) of each unit will normally be the Executive Officer who will appoint an assistant Security Officer for Personal and Physical Security. In Recruit School the Assistant Security Officers are:

- Physical Security: s47E(c) (DO Shipp Division)
- Personal Security: s47E(c) (Command Building)

JOINT MILITARY POLICING UNIT JMPU

The Joint Military Policing Unit (JMPU) is to provide law enforcement on RAN Establishments. The JMPU is a tri-service unit from Navy, Army and Air Force. On HMA Ships the NPC's take on this role. At RAN establishments' physical security is supplemented by contracted security firms.

ALL PERSONNEL

Every member of the ADF and employee of the Department of Defence has an individual responsibility to acquire and maintain security awareness. This responsibility must be clearly explained to all new arrivals in units, and repeated frequently as part of the security education program.

A Minor security incident is an accidental or unintentional action involving failure to observe protective security policy mandatory requirements or procedures within the Defence Security Principles Framework. Examples include:

Access passes or identification documents lost or left insecure; or security classified material not properly secured or stored.

IDENTIFY A SECURITY INCIDENT

A security incident is an occurrence, which results, or may result, in negative consequences for the security of Defence.

Incidents are classified as Minor, Major or Reportable Major Security Incidents.

a. A **Minor** security incident is an accidental or unintentional action involving failure to observe protective security policy mandatory requirements or procedures within the Defence Security Principles Framework. Examples include:

b. Access passes or identification documents lost or left insecure; or security classified material not properly secured or stored.

c. A **Major** security incident is any deliberate, negligent or reckless action that leads, or could lead, to the loss, damage, corruption or disclosure of Official Information or assets.

d. A **Reportable Major** security incident is any occurrence requiring reporting to the Australian Security Intelligence Organisation (ASIO) as defined I the ASIO Act (1979), including espionage or suspected espionage.

IDENTIFY A SECURITY INCIDENT

ACTION TO BE TAKEN

When working in secret or top secret environments you may discover unsecured documents, containers or compartments/rooms. On discovering any security incident you should:

- Remain with the unsecured material or compartment.
- Report the incident to a person in authority. Normally the USO and after hours the OOD through the QM.

LOOSE TALK AT RECRUIT SCHOOL

At Recruit School, some common security breaches are made. This is due to discussing topics such as:

a. Actual level of training with Austeyr including (but not limited to):

(1) Where you fire the weapon;

(2) Ammunition detail; and

(3) What your capability is.

b. Number of personnel on duty;

c. Any information when you're unsure who you're talking to; and

d. Anything regarding your security clearance.

"No unauthorised public comment is to be made at any time, e.g. comments to media".

SECURITY ROUNDS

ANNEX 14F

HMAS HOBART DAILY SECURITY ROUNDS REPORT

Day and Date: **HARBOUR / CRUISING /DEFENCE**

To be retained for two months then destroyed

Personnel Responsible	Name	0800 To 0900	1400 To 1500	Completion of work rounds	1900 To 2000	2000 To 2100	2100 To 2200	2200 To 2300	2300 To 2359	0001 To 0100	0100 To 0200	0200 To 0300	0300 To 0400	0400 To 0500	0500 To 0600	0600 To 0700
OOD																
DPO/DWC																
EOOD																
LSMT																
ABMT																
LSET																
ABCIS																
QM																
QMA																

MUSTERS / CHECKS

DEPARTMENT	CORRECT (Yes/No)	SIGNATURE	REMARKS
Ops Room ACCM Muster			
COMCEN ACCM Muster			

COMPARTMENTS LEFT OPEN AT COMPLETION OF WORK

Compartment	Found By	User	Time found	Time Secured	Secured by	Signature

OOD:	**XO:**	**CO**

Exercise 1 - Match the colour and level of damage to the security classification.

Classification	*Identification Colour*	*Consequence*
Top Secret	**Grey**	Damage
Secret	**White**	Limited Damage
Protected	**Red**	Insignificant Damage
Sensitive: Official	**Blue**	Serious Damage
Official	**Yellow**	No Damage
Unofficial	**Salmon**	Exceptional grave damage

Exercise 2 – Fill in the blanks

Expand the Exploitable Weaknesses Acronym

P _____

R _____

I _____

M _____

E _____

D _____

List the four levels of personnel security clearances

_____

_____

_____

_____

List and define the three SAFE BASE levels

_____

_____

_____

_____

_____

List the three Information Management Markers (IMM)

_____

_____

_____

_____

_____

SECURITY

MODULE 07

SERVICE
COURAGE
RESPECT
INTEGRITY
EXCELLENCE

SECURITY EXPERIENCE

Do you have any previous experience with security?

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1 Contribute to the maintenance of RAN security
  - 7.1.1 Maintain protective security
    - 7.1.1.1 Define national security
    - 7.1.1.2 Identify major threats to national security
    - 7.1.1.3 Define protective security
    - 7.1.1.4 Define the “Security In Depth” principal

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1.2 Maintain Physical Security
  - 7.1.2.1 Define physical security
  - 7.1.2.2 State measures used to maintain physical security
  - 7.1.2.3 State purpose of the SAFEBASE alert system
  - 7.1.2.4 List close of business routines

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1.3 Maintain Personnel Security
  - 7.1.3.1 Define personnel security
  - 7.1.3.2 List measures used to maintain personnel security
  - 7.1.3.3 State an individual's responsibilities to maintain personnel security
  - 7.1.3.4 List exploitable weaknesses in personal character

REFERENCES

- Defence Security Principles Framework
- Protective Security Policy Framework
- Information Security Manual
- Class Standing Orders
- (Individual Platforms i.e. DDG and LHD)
- Section Security Orders

NATIONAL SECURITY

- The definition of National security is ‘A term used to describe the safety of the nation from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia’s defence system, and acts of foreign interference’.

THE THREAT

- Trusted Insider
- Foreign Intelligence Services
- Terrorism
- Issue Motivated Groups
- THE BELIEF THAT THERE IS NO THREAT!

INFORMATION SOUGHT

- Did You Know?

  The most sought after Defence information by Foreign Intelligent Services often relates to:

  - Emerging Technologies
  - Aerospace
  - Communications
  - Electronics
  - Weapons Developments

PROTECTIVE SECURITY

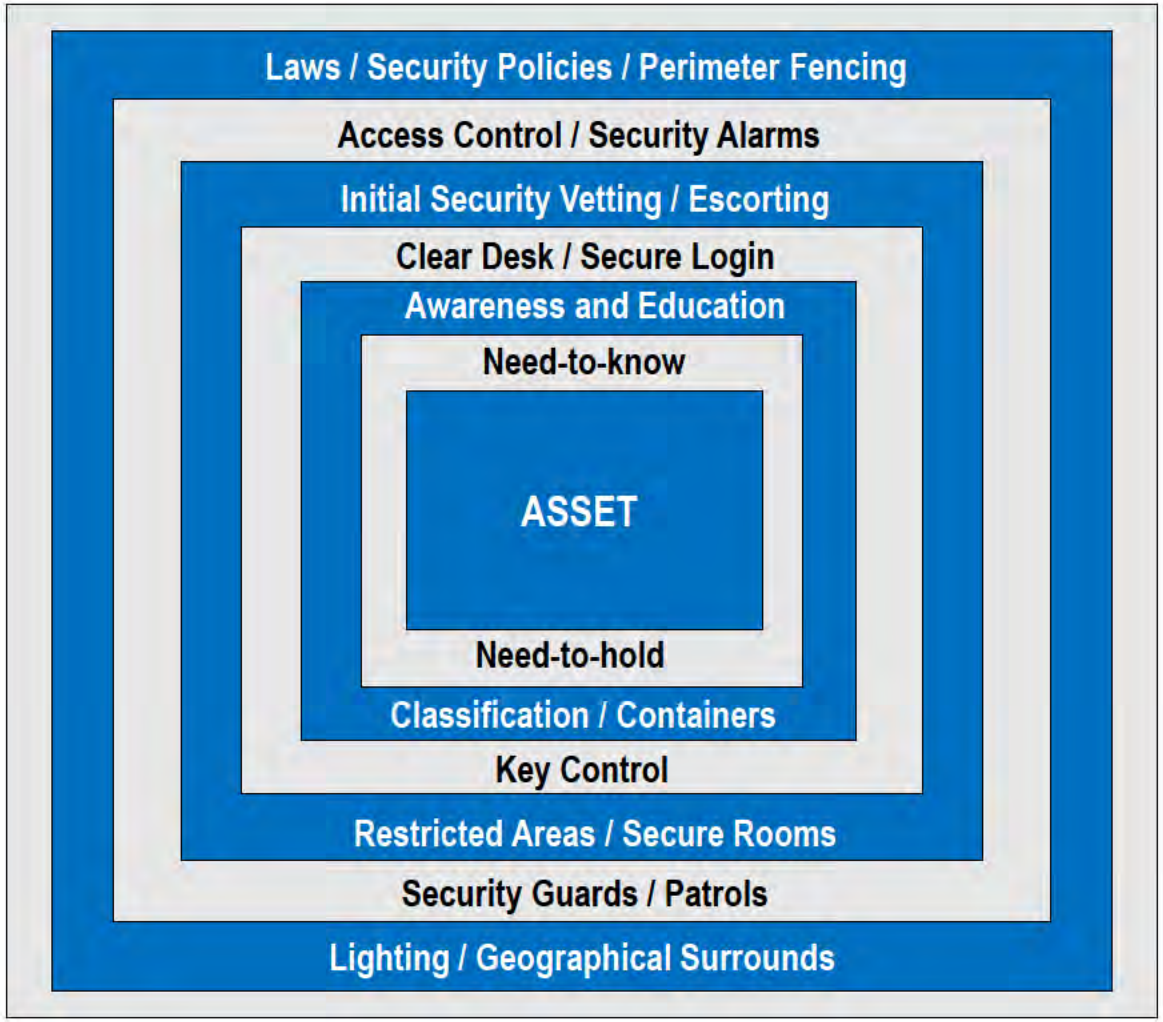
- Protective security is the total concept of Information, Personnel, Physical and Information & Communications Technology (ICT) security.

SECURITY-IN-DEPTH-PRINCIPLE

EXERCISE

Close your books

SECURITY-IN-DEPTH-PRINCIPLE



PHYSICAL SECURITY - PRINCIPLE

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

PHYSICAL SECURITY - RATIONALE

- Application of physical security measures consistent with whole of Government requirements will:
  - Ensure a secure physical environment for storage and handling of official resources.
  - Facilitate sharing of information and assets across Government, with allies and persons engaged under contract.
  - Maintain a safe and secure working environment for Defence personnel and persons engaged under contract.

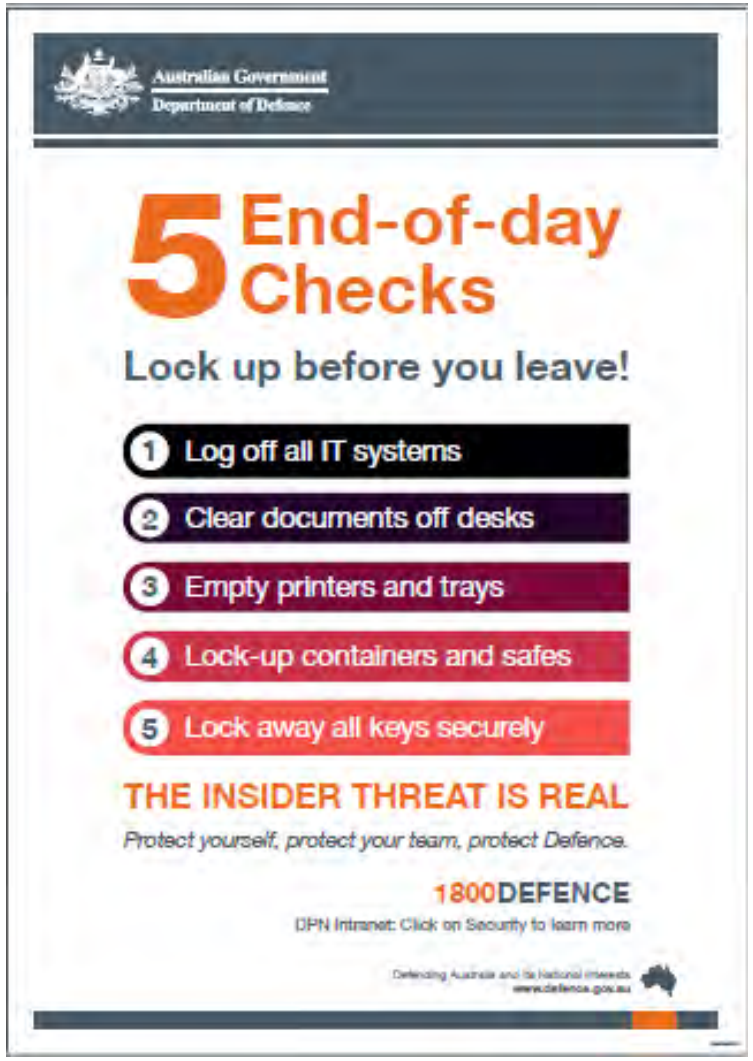
PHYSICAL SECURITY MEASURES

- Perimeter fences and gates
- Guard posts
- External and internal facility guard patrols
- External and internal CCTV systems
- Security alarm systems
- Other access control measures such as cipher locks and biometric systems
- Security Keys
- Security Containers
- SAFEBASE alert system

PHYSICAL SECURITY

- Defence Security Passes
  - You must wear this pass at all times in the Defence environment and it is your responsibility to:
    - wear your pass externally on your clothing
    - remove your pass from sight when leaving the premises to avoid attracting attention
    - always wear your pass on Defence premises.

PHYSICAL SECURITY



SERVICE
COURAGE
RESPECT
INTEGRITY
EXCELLENCE

SAFEBASE SECURITY ALERT SYSTEM

PERSONNEL SECURITY

SERVICE
COURAGE
RESPECT
INTEGRITY
EXCELLENCE

PERSONNEL SECURITY

- The taking of responsible and practical measures to ensure that only Loyal, Reliable and Trustworthy persons who have an established need are permitted access to classified Defence information and assets

SECURITY CLEARANCES

- The four levels of personnel security clearances are:
  - BASELINE
  - NEGATIVE VETTING – LEVEL 1 (NVL1)
  - NEGATIVE VETTING – LEVEL 2 (NVL2)
  - TOP SECRET POSITIVE VETTING (TSPV)

PERSONNEL SECURITY MEASURES

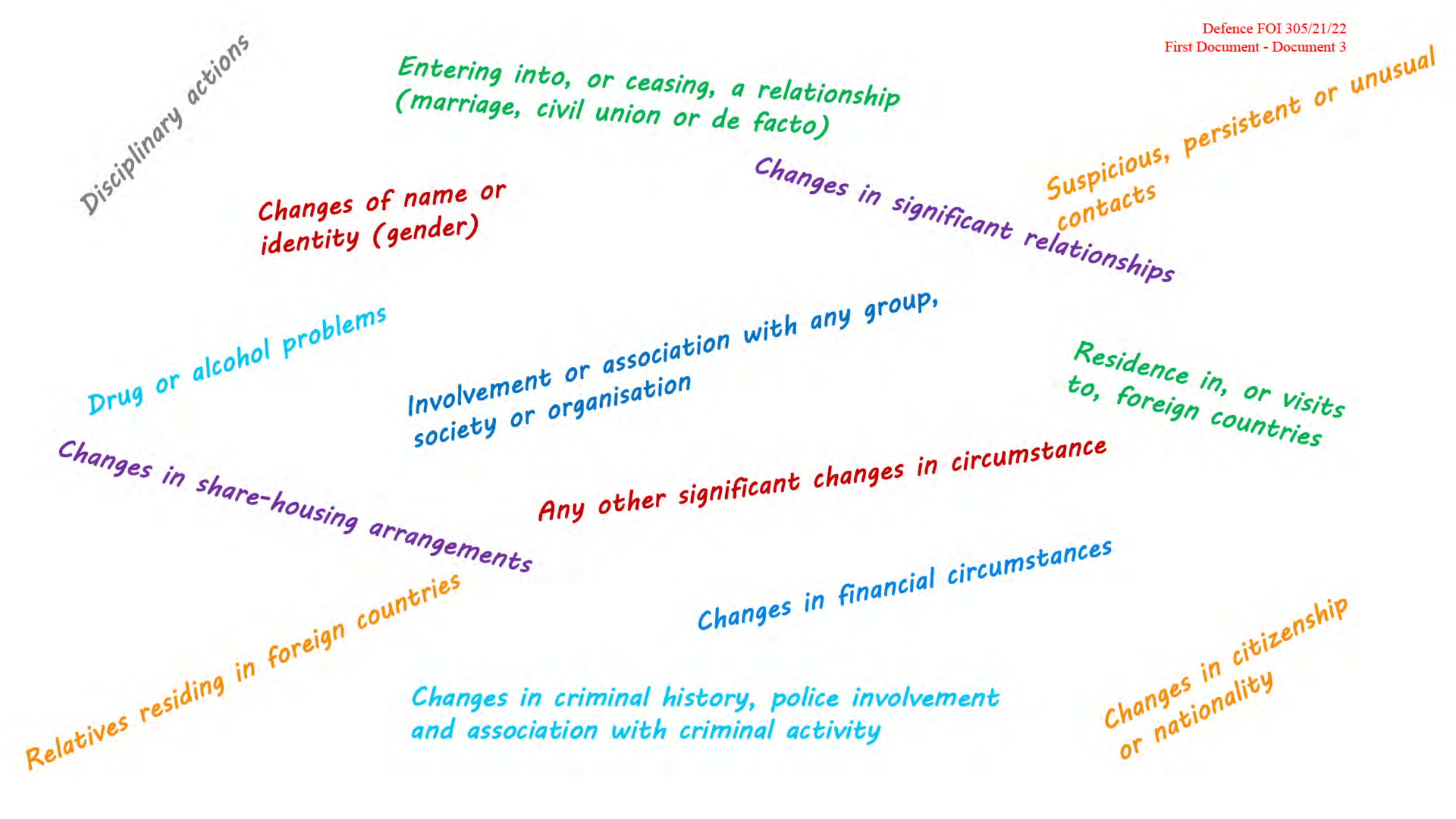
- Security vetting and clearances
- Security education
- Control of access /need to know
- Monitoring of overseas travel
- Punitive measures

PERSONNEL SECURITY
CHANGE IN CIRCUMSTANCES

- If you have a change in personal circumstances you must inform AGSVA.

  This can be done:

  - Online via the ePack system (using your security clearance ePack login details)
  - By downloading an SVA003 from the 'Resources' page of the AGSVA website.


Disciplinary actions
Entering into, or ceasing, a relationship (marriage, civil union or de facto)
Changes of name or identity (gender)
Changes in significant relationships
Suspicious, persistent or unusual contacts
Drug or alcohol problems
Involvement or association with any group, society or organisation
Residence in, or visits to, foreign countries
Changes in share-housing arrangements
Any other significant changes in circumstance
Relatives residing in foreign countries
Changes in financial circumstances
Changes in criminal history, police involvement and association with criminal activity
Changes in citizenship or nationality

EXPLOITABLE WEAKNESSES

- Promiscuity
- Revenge
- Ideology
- Money
- Ego
- Drugs

PRIMED is for Compromise

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1 Contribute to the maintenance of RAN security
  - 7.1.1 Maintain protective security
    - 7.1.1.1 Define national security
    - 7.1.1.2 Identify major threats to national security
    - 7.1.1.3 Define protective security
    - 7.1.1.4 Define the “Security In Depth” principal

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1.2 Maintain Physical Security
  - 7.1.2.1 Define Physical Security
  - 7.1.2.2 State measures used to maintain physical security
  - 7.1.2.3 State purpose of the SAFEBASE alert system
  - 7.1.2.4 List close of business routines

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1.3 Maintain Personnel Security
  - 7.1.3.1 Define Personnel Security
  - 7.1.3.2 List measures used to maintain Personnel Security
  - 7.1.3.3 State an individual's responsibilities to maintain Personnel Security
  - 7.1.3.4 List exploitable weaknesses in personal character

QUESTIONS?

SECURITY

MODULE 07, Part 2

SERVICE
COURAGE
RESPECT
INTEGRITY
EXCELLENCE

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1.4 Define Information Security
  - 7.1.4.1 Define information security
  - 7.1.4.2 Define the Australian Government Security Classification System
  - 7.1.4.3 Identify Information Management Markers
  - 7.1.4.4 Describe the principles of need to know and need to hold

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1.5 Define Information, Communication and Technology (ICT) Security
  - 7.1.5.1 Define ICT security
  - 7.1.5.2 State measures to maintain ICT Security

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1.6 Conduct Security Rounds
  - 7.1.6.1 Define the RAN security organisation
  - 7.1.6.2 Define the role of personnel within the security organisation
  - 7.1.6.3 Identify a security breach
  - 7.1.6.4 Describe the actions to be taken on discovering a security breach
  - 7.1.6.5 Conduct security rounds IAW relevant SSO's

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.

AUSTRALIAN GOVERNMENT SECURITY CLASSIFICATIONS

- There are Six Australian Government Security Classifications:
  - UNOFFICIAL
  - OFFICIAL
  - OFFICIAL: SENSITIVE
  - PROTECTED
  - SECRET
  - TOP SECRET

AUSTRALIAN GOVERNMENT SECURITY CLASSIFICATIONS

Protective Markers and Classifications

UNOFFICIAL	E.g. an invitation to a birthday party
OFFICIAL	E.g. publicly accessible page on the Defence website
OFFICIAL: Sensitive	E.g. procurement details for a Defence Industry project
PROTECTED	E.g. weapons movement report
SECRET	E.g. operational military plans
TOP SECRET	E.g. intelligence report on a foreign agency

OFFICIAL VS UNOFFICIAL

All information related to your work for Defence is **OFFICIAL** information.

Examples may include:

- Hand written notes that you write at a Defence meeting
- An email to a work colleague about a Defence matter
- Information prepared for public access or circulation, such as websites or Frequently Asked Questions

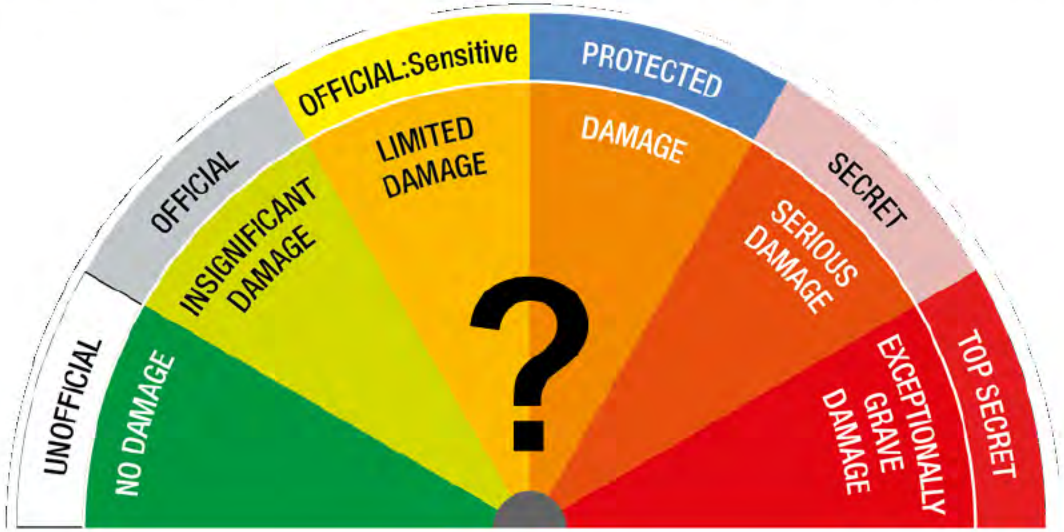
Information relating to your social or home life is **UNOFFICIAL** information.

Examples may include:

- An invitation to meet someone at the gym
- Calling your mechanic about a car service
- Arranging tennis coaching for the weekend.

ASSESS THE DAMAGE

- When handling classified information, think to your self how much damage would it cause if the information was leaked or made public, what damage could it cause to people, organisations or government?



IMPACT LEVELS

TOP SECRET

If leaked or made public, there would be exceptionally grave damage to people, organisations or government

IMPACT LEVELS

SECRET

If this information was leaked or made public, there would be serious damage to people, organisations or government.

IMPACT LEVELS

PROTECTED

If this information was leaked or made public, it would damage people, organisations or government.

IMPACT LEVELS

OFFICAL: Sensitive

If this information was leaked or made public, there would be limited damage to people, organisations or government.

IMPACT LEVELS

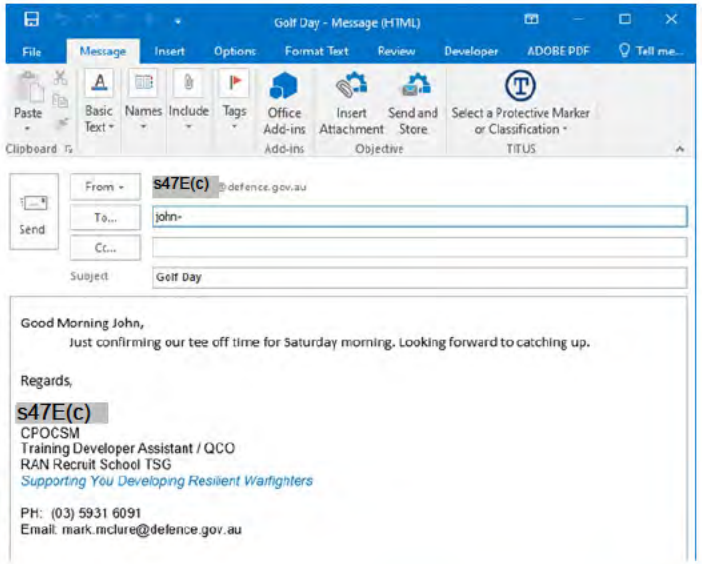
OFFICIAL

If this information was leaked or made public, there would be insignificant damage to people, organisations or government

IMPACT LEVELS

UNOFFICAL

Information is not part of your work for Defence so would cause no damage.



INFORMATION MANAGEMENT MARKERS

- Information Management Markers (IMM)
  - Legal Privilege
  - Legislative Secrecy
  - Personal Privacy

NOTE: IMMs can be applied to information assessed as: OFFICIAL: Sensitive or above.


SECRET//AUSTEO
Legal privilege

Subject: Examples

Legal privilege
SECRET//AUSTEO

NEED TO KNOW

- The NEED-TO-KNOW principle requires that access to classified information which is limited to those who are appropriately cleared and need to use it for their work.

NEED TO HOLD

- The NEED-TO-HOLD principle requires that classified documents or material are to be held only by those individuals or units who have a need for immediate access to them.

LOOSE OR UNGUARDED TALK

- The following are examples of subjects not to be discussed or revealed to persons other than service personnel with a need to know:
  - All classified information.
  - Movements of HMA Ships or Personnel.
  - Details / Results of operations or equipment trials.
  - Capabilities of ships/equipment.
  - Technical details of weapons/equipment.
  - Identification of key personnel.

INFORMATION & COMMUNICATION TECHNOLOGY (ICT) SECURITY

ICT SECURITY

- Information and communication technology (ICT) security is about protecting information stored and transmitted in electronic format. This includes security measures concerning:
  - Computers (Including Internet and Social Media)
  - Defence Voice Environment
  - Phones
  - Multi Function Devices
  - Cyber and multimedia

ICT SECURITY MEASURES

- Defence has significant measures in place to ensure ICT Security depending on the method. Examples are:
  - Procedures and Processes
  - Classifying Information
  - Labelling of Devices and Information
  - Controlling Access
  - Classified Material Registers
  - Securing ICT Equipment and Media

PROCEDURES AND PROCESSES

- To ensure adequate protection of ICT, there will be higher level and local procedures and processes to be followed. Generally you will not be provided access until you have completed the process to have access to a system.
- An example is reading and acknowledging the DPN policy as part of gaining access to that network. Additionally, having the appropriate security clearance, a sponsor to apply on your behalf and access.

CLASSIFICATION OF ICT

- To ensure ICT is used, handled and stored appropriately, equipment is classified to the level of the highest classification to be used. Example is:
  - The Defence Protected Network (DPN) cannot be used to store Secret information.

LABELLING OF EQUIPMENT, DEVICES AND INFORMATION

- To ensure equipment and media are handled correctly they will be clearly labelled. This will include:

CONTROLLING ACCESS

- Access to ICT equipment and media is controlled by:
  - Authorised personnel entrance lists
  - Access to applications
  - Passwords
  - Combinations to compartments or safes
  - Encryption
  - Handling
  - Sanitising

CLASSIFIED MATERIAL REGISTERS

- To ensure ICT is always accounted for, a register is maintained that records where information is held and who is holding it.
- As you progress in your career and have access to higher level information you will be provided instruction on theses procedures.

SECURING ICT EQUIPMENT AND MEDIA

- When ICT equipment is not in use it must be secured in an approved container, vault or compartment.

RAN SECURITY ORGANISATION

SERVICE
COURAGE
RESPECT
INTEGRITY
EXCELLENCE

RAN SECURITY ORGANISATION

Secretary of Defence

Chief of Defence Force

Chief Security Officer

Directorate of Policing and Security – Navy (DPS-N)

Unit Security Officer (USO)

Joint Military Policing Unit (JMPU)

SECURITY INCIDENT

- A security incident is an occurrence which results, or may result, in negative consequences for the security of Defence
- Incidents are classified as Minor, Major or Reportable Major Security Incidents.

MINOR

MAJOR

MAJOR REPORTABLE

SECURITY INCIDENT (BREACH)

- When working in secret or top secret environments you may discover unsecured documents, containers or compartments/rooms. On discovering any security breach you should:
  - Remain with the unsecured material or compartment.
  - Report the incident to a person in authority. Normally the USO during working hours and after hours the OOD through the QM.

NOTE: At no time are you to leave the material or compartment unattended.

LOOSE TALK

- At Recruit School, some common security incidents that occur are topics such as:
  - Actual level of training with Austeyr including (but not limited to):
    - Where you fire the weapon
    - Ammunition detail
    - What your capability is
  - Number of personnel on duty
  - Any information when you're unsure who you're talking to
  - Anything regarding your security clearance

SECURITY ROUNDS

ANNEX 14F

HMAS HOBART DAILY SECURITY ROUNDS REPORT

Day and Date: **HARBOUR / CRUISING /DEFENCE**

To be retained for two months then destroyed

Personnel Responsible	Name	0800 To 0900	1400 To 1500	Completion of work rounds	1900 To 2000	2000 To 2100	2100 To 2200	2200 To 2300	2300 To 2359	0001 To 0100	0100 To 0200	0200 To 0300	0300 To 0400	0400 To 0500	0500 To 0600	0600 To 0700
OOD																
DPO/DWC																
EOOD																
LSMT																
ABMT																
LSET																
ABCIS																
QM																
QMA																

MUSTERS / CHECKS

DEPARTMENT	CORRECT (Yes/No)	SIGNATURE	REMARKS
Ops Room ACCM Muster			
COMCEN ACCM Muster			

COMPARTMENTS LEFT OPEN AT COMPLETION OF WORK

Compartment	Found By	User	Time found	Time Secured	Secured by	Signature

OOD:	XO:	CO

YOUR RESPONSIBILITY

REMEMBER!!!!

Security is everyone's responsibility whether on duty or not.

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1.4 Define Information Security
  - 7.1.4.1 Define information security
  - 7.1.4.2 Define the Australian Government Security Classification System
  - 7.1.4.3 Identify Information Management Markers
  - 7.1.4.4 Describe the principles of need to know and need to hold

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1.5 Define Information, Communication and Technology (ICT) Security
  - 7.1.5.1 Define ICT security
  - 7.1.5.2 State measures to maintain ICT Security

LEARNING OUTCOMES & ASSESSMENT CRITERIA

- 7.1.6 Conduct Security Rounds
  - 7.1.6.1 Define the RAN security organisation
  - 7.1.6.2 Define the role of personnel within the security organisation
  - 7.1.6.3 Identify a security breach
  - 7.1.6.4 Describe the actions to be taken on discovering a security breach
  - 7.1.6.5 Conduct security rounds IAW relevant SSO's

	ROYAL AUSTRALIAN NAVY (RAN Recruit School)
	INSTRUCTOR GUIDE **MODULE 7** **SECURITY**

Introduction

1. This RAN Recruit School (RS) document is approved and issued for all RS instructing staff.

2. All changes must be authorised by the Course Implementation Officer Recruit School (CIO-RS) or designated representative and will be effective upon promulgation. Suggested improvements are to be forwarded to the CIO-RS.

Version Control Metadata

Title:	**101217 General Service Duties Recruit Course – LMG Module 7 Secruity**
Author	RS (TSG)
Approver	TA-ITLM
Version Number	V1752479
Date of Approval/amendment	Feb 21
Next review date:	Feb 22
Coverage	LMG for GSDR Module 7
E- file location	Recruit School Intranet Home Page

s47E(c)

Digitally signed by s47E(c)
Date: 2021.02.03 14:55:00 +11'00'

s47E(c)
LEUT, RAN
Course Implementation Officer
RAN Recruit School

03 Feb 21

Facilitators

New facilitators are to follow the full instructions of this guide when first instructing the course. Suggestions for amendments must be endorsed before use.

Experienced facilitators may deliver the content using different delivery methods, as long as:

The Learning Outcomes (LOs), Assessment Criteria (AC) and core content are covered.

An effective lesson plan has been designed (i.e. the events of instruction have been adequately covered).

Note: Facilitators are considered to be 'experienced' once they have instructed the module at least twice and their supervisor is comfortable that they can deliver content to the required level. This agreement is to be recorded and stored with staff management records.

Context

SLO 7.1.1 Maintain Protective Security
SLO 7.1.2 Maintain Physical Security
SLO 7.1.3 Maintain Personnel Security
SLO 7.1.4 Maintain Information Security
SLO 7.1.5 Maintain Information, Communication and Technological Security
SLO 7.1.6 Conduct Security Rounds

Assessment Criteria

AC 7.1.1.1 Define national security
AC 7.1.1.2 Identify major threats to national security
AC 7.1.1.3 Define Protective Security
AC 7.1.1.4 Describe the "security in depth" principle
AC 7.1.2.1 Define physical security
AC 7.1.2.2 State measures used to maintain physical security
AC 7.1.2.3 State the purpose of the SAFEBASE alert system
AC 7.1.2.4 List close of business routines
AC 7.1.3.1 Define personnel security
AC 7.1.3.2 List measures used to maintain personnel security
AC 7.1.3.3 State an individual's responsibilities to maintain personnel security
AC 7.1.3.4 List exploitable weaknesses in personal character
AC 7.1.4.1 Define information security
AC 7.1.4.2 Identify the Australian Government Security Classification System markings
AC 7.1.4.3 Identify Dissemination Limiting Markers
AC 7.1.4.4 Describe the principles of need to know and need to hold
AC 7.1.5.1 Define ICT security
AC 7.1.5.2 State measures to maintain ICT security
AC 7.1.6.1 Define the RAN security organisation
AC 7.1.6.2 Describe the role of personnel within the security organisation
AC 7.1.6.3 Identify a security breach
AC 7.1.6.4 Describe the actions to be taken upon discovering a security breach
AC 7.1.6.5 Conduct security rounds IAW relevant SSOs

Preparation and Resources

Potential issues

Class sizes do sometimes exceed 24 when large divisions are recruited. This affects maximum capacity of classroom and access to desks/computers.

Resources

Course materials

To facilitate this course you will need:

GSDR Module Book (Already issued to students)

Instructor Guide for LO 7.1

Slide presentations for LO 7.1

Module Training Aid Box (Contains secret folder, I-phone & charger, secret folder, Top Secret document and Tablet)

Handouts per trainee

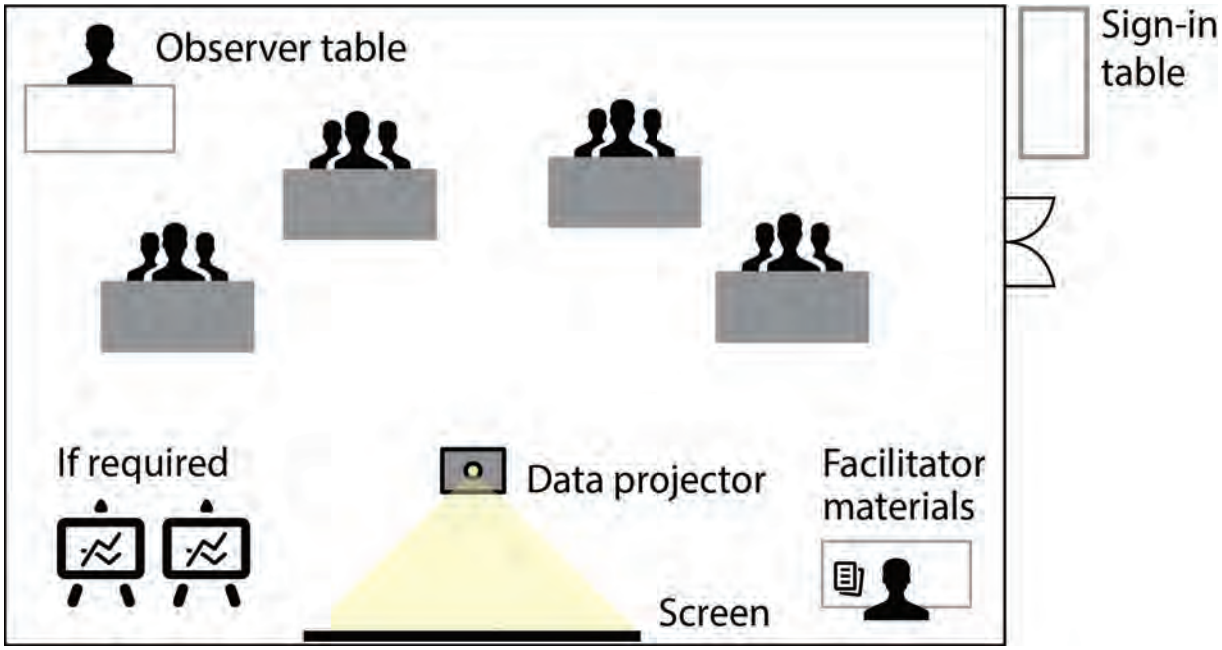
Nil

Student Requirements

On sitting down students will need to log in to ADELE and their Defence email. Students may follow the lesson on ADELE through Powerpoint and will require access to email to conduct an exercise during the instruction.

Learning Space

The learning space could be set up in either café style or in a U-shape. Consider café style to allow more flexibility and interaction.



Equipment

Classroom with seating for 24 students

Whiteboard markers

Whiteboard

Data projector

Facilitator computer with DPN access

Projection screen

Lectern

Delivery Method Icons

This table explains the icons used within this guide.

Icon	Name	Description
	Group activity	Discussion/activity in small groups of 2 or 3.
	Display slide	PowerPoint presentation
	Handout	Additional information not in reference material Instructions and source material for an activity
	Question	Question/s to ask students
	Alert	Alert students to key learning point
	Module Book	Refer students to module book or fill in blanks etc.

Module 7 - SECURITY		Timing Total: 120 Minutes
Timing	Content	Notes
		**Slide 01 – Title** Security

Script for facilitator: (Teaching / learning points)

The security module will be delivered in two parts both of one hour duration. Content is available in the GSDR Workbook and ADELE. You may ask questions at any stage throughout the lesson.

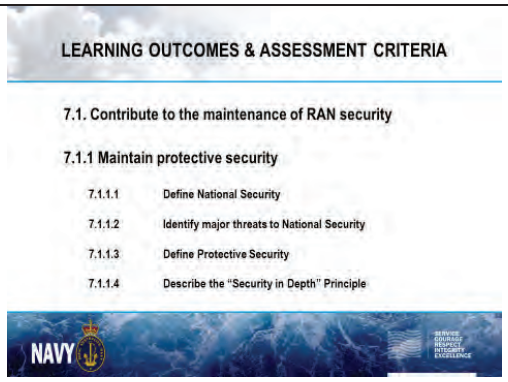
Timing	Content	Notes
2 mins		**Slide 02 – Previous Experience**

Script for facilitator: (Teaching / learning points)

Gain an understanding of class previous experience and current knowledge.

? Ask students what experiences if any, they have had with security either in a military or civilian context.

If required prompt them with the security requirements at the airport, ID passes for specific work places and access to sites. Keep these answers in mind to refer back to as examples if required when facilitating each SLO.

Timing	Content	Notes
3 mins		**Slide 03-05 – LO, SLO and AC**

Script for facilitator: (Teaching / learning points)

Read LO, SLO and AC for entire module.

LO Contribute to the maintenance of RAN Security

SLO 7.1.1 Maintain Protective Security
- AC 7.1.1.1 Define national security
- AC 7.1.1.2 Identify major threats to national security
- AC 7.1.1.3 Define Protective Security
- AC 7.1.1.4 Describe the "security in depth" principle

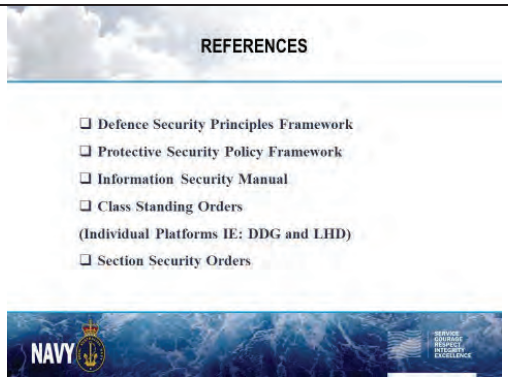
(Next Slide)

SLO 7.1.2 Maintain Physical Security
- AC 7.1.2.1 Define physical security
- AC 7.1.2.2 State measures used to maintain physical security
- AC 7.1.2.3 State the purpose of the SAFEBASE alert system
- AC 7.1.2.4 List close of business routines

(Next Slide)

SLO 7.1.3 Maintain Personnel Security
- AC 7.1.3.1 Define personnel security
- AC 7.1.3.2 List measures used to maintain personnel security
- AC 7.1.3.3 State an individual's responsibilities to maintain personnel security
- AC 7.1.3.4 List exploitable weaknesses in personal character

(Next Slide)

Timing	Content	Notes
4 mins		💻 **Slide 06 – References**

📄 Script for facilitator: (Teaching / learning points)

The references are:

Defence Security Principles Framework (DSPF)

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

Protective Security Policy Framework (PSPF)

The Protective Security Policy Framework (PSPF) assists Australian Government entities to protect their people, information and assets, both at home and overseas.It sets out government protective security policy and supports entities to effectively implement the policy across governance, information, personal and physical security.

Information Security Manual (ISM)

The purpose of the ***Australian Government Information Security Manual*** (ISM) is to outline a cyber security framework that organisations can apply, using their risk management framework, to protect their systems and information from cyber threats.

Class Standing Orders

Class and Ships Standing Orders will delegate security orders that are applicable for the effective running of the platform and overall ships company.

Section Security Orders

Within each ship or establishment there will be specific Section Security Orders for sections with Secret or Top Secret classifications.

NOTE: The five listed references are readily available to you and were used for this lesson; however, the number of references relating to security are extremely vast.

Next

Timing	Content	Notes
5 mins		**Slide 07 – National Security** AC 7.1.1.1-Define National Security

Script for facilitator: (Teaching / learning points)

Built Slide

National Security
Read definition of National Security

'National security is a term used to describe the safety of the nation from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence systems, and acts of foreign interference'.

Have students fill in blanks in workbook, highlighted in red.

Next Slide

Timing	Content	Notes
6 mins		**Slide 08 – Threats to Security** AC 7.1.1.2

Script for facilitator: (Teaching / learning points)

Built Slide

While some security threats are found to be intentional (e.g. espionage), most incidents are not. They are actually a result of poor security practices in the workplace. This means each one of us have a significant opportunity to combat security threats on a daily basis.

It is also important to understand that although there are many different types of security threats, there are only five common sources for those threats.

Next

- **Trusted Insider** - Internal threats come in a variety of forms including the accidental disclosure of sensitive information; disgruntled staff looking to get back at Defence; and staff that are specifically targeted by external threat sources.

Next

- **Foreign Intelligence Services** - Foreign Intelligence Services want to discover our Defence capabilities.

Next

- **Terrorism** - People that use or threaten to use violence against individuals or property in an attempt to coerce or intimidate governments, societies or communities to achieve ideological, political or religious objectives.

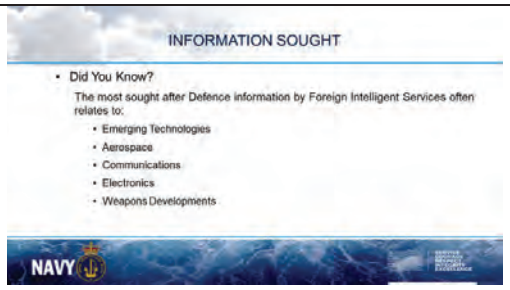
Next

- **Issue Motivated Groups** - An issue motivated group can be defined as a collection of activists with a common ideology that engages in political activities but is not a registered political party. However, extreme groups can engage in ‘direct action’, such as blockading Defence facilities or trespassing into Defence exercise areas even personal assaults.

Next

- **THE BELIEF THAT THERE IS NO THREAT**.

Next Slide

Timing	Content	Notes
9 mins		**Slide 09 – Information Sought** No AC

Script for facilitator: (Teaching / learning points)

Not Assessment Criteria

DID YOU KNOW

- **The most sought after Defence information by Foreign Intelligence Services often relates to:**
  - **Emerging Technologies**
  - **Aerospace**
  - **Communications**
  - **Electronics**
  - **Weapons Developments**

Have students take 30 seconds to think about what rate they have joined as and if they will have access to this type of information in the future.

Ask Students if they think they do?

Utlising the Pose, Pause, Pounce method obtain class answers.

Next Slide

Timing	Content	Notes
10:30 mins		**Slide 10 – Definition of Protective Security** AC 7.1.1.3

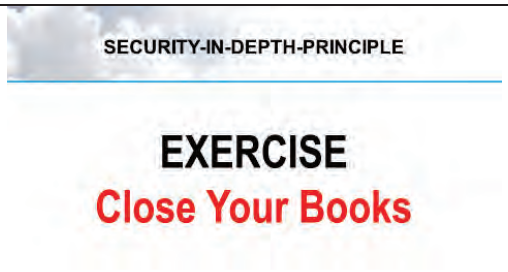
Script for facilitator: (Teaching / learning points)

Protective security is the total concept of information, personnel, physical and information & communications, technology (ICT) security.

Explain that we will go through the key points of Physical, Personnel and ICT in detail throughout the module.

Recruits need to highlight this in the Module Book.

Next Slide

Timing	Content	Notes
12 mins		**Slide 11 – Security-In-Depth Principle** AC 7.1.1.4

Script for facilitator: (Teaching / learning points)

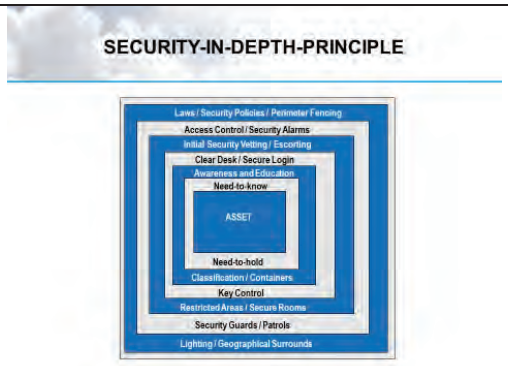
Presenter Information

Built Slide

EXERCISE: Students are to close books and use spare paper. Divide class into groups of three.

Ask students to note down all the measures in place at HMAS *Cerberus* to protect the Recruit School Armoury. Time allowed 2 minutes. Leave blank while students are writing down answers.

Next Slide

Timing	Content	Notes
16 mins		**Slide 12 – Security-In-Depth Principle** AC 7.1.1.4

Script for facilitator: (Teaching / learning points)

Display Slide and using the diagram working from the outside in ask students what measures they have observed that are in place for each measure.

Next

Laws / Security Policies / Perimeter Fencing - Lighting / Geographical Surrounds

Next

Access Control / Security Alarms - Security Guards / Patrols

Next

Initial Security Vetting / Escorting - Restricted Areas / Secure Rooms

Next

Clear Desk / Secure Login - Key Control

Next

Awareness and Education - Classification / Containers

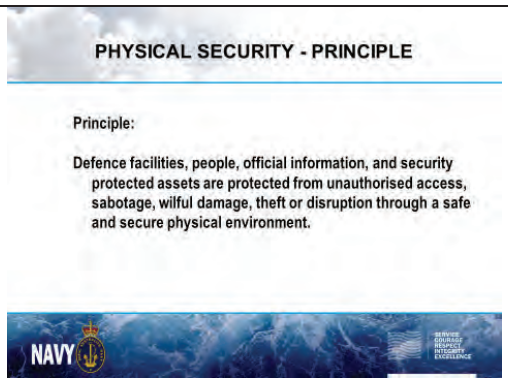
Next

Need-to-know - Need-to-hold

A series of protective barriers are more robust than a single line of defence.

- Security should be layered so that the asset is not reliant on any one measure for protection.

Open Books - Next Slide

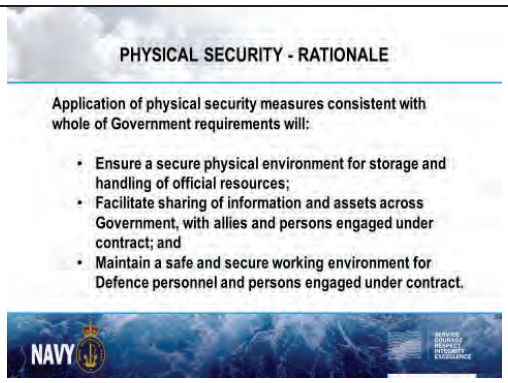
Timing	Content	Notes
18 mins		**Slide 13 Physical Security Principle** AC 7.1.2.1

Script for facilitator: (Teaching / learning points)

Physical security is broken into the security principle and security rationale.

The security principle defines 'Defence facilities, people, official information, and security protected assets are protected from unauthorised access, sabotage, wilful damage, theft or disruption through a safe and secure physical environment.

Next Slide

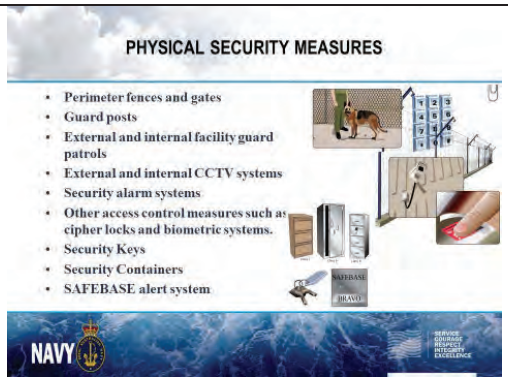
Timing	Content	Notes
19 mins		**Slide 14 – Physical Security - Rationale** AC 7.1.2.1

Script for facilitator: (Teaching / learning points)

The physical security rationale is the application of physical security measures consistent with whole of Government requirements, it will:

- Ensure a secure physical environment for storage and handling of official resources;
- Facilitate sharing of information and assets across Government, with allies and persons engaged under contract; and
- Maintain a safe and secure working environment for Defence personnel and persons engaged under contract.

Next Slide

Timing	Content	Notes
21 mins		**Slide 15 – Physical Security Measures** AC 7.1.2.2

Script for facilitator: (Teaching / learning points)

Physical Security Measures include:

- Perimeter fences and gates
- Guard posts / access points
- External and internal facility guard patrols
- External and internal CCTV systems
- Security alarm systems
- Other access control measures such as cipher locks and biometric systems.
- Security Keys
- Security Containers
- SAFEBASE Alert System

Highlight that all these measures are onboard HMAS *Cerberus* and any other areas from your own experience if applicable.

Next Slide

Timing	Content	Notes
25 mins		**Slide 16 – Security Passes** No AC

Script for facilitator: (Teaching / learning points)

Presenter Information

There are approved ways in which you must wear your Defence pass such as wearing it clearly visible, displayed above your waist.

Show where on yourself you are wearing yours and the other places it may be worn.

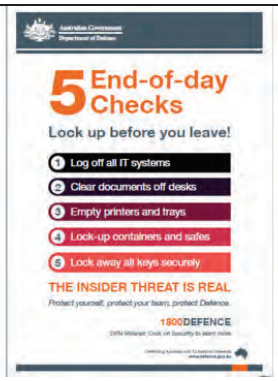
As you can see by the slide there are several different types of passes that you will see. Issuing of passes is the responsibility of the contractor employed at each defence site.

These passes may be for Defence Personnel, civilians, contractors, Family (Such as a Husband or wife of a serving member), foreign military or a visitor. Visitor passes will be annotated with 'ESCORTED' meaning that person is to be with a pass holder at all times.

? What actions would you take if you came across someone in Recruit School who was by themselves displaying a visitor pass that said 'ESCORTED'?

NOTE: Passes are not be worn or displayed when outside of Defence Premises.

Next Slide

Timing	Content	Notes
30 mins		**Slide 17 – End of Day Checks** AC 7.1.2.4

Script for facilitator: (Teaching / learning points)

Before securing each day the following checklist is to be followed:

- Log off all IT Systems
- Clear documents off desks
- Empty printers and trays
- Lockup containers and safes
- Lock away all keys securely

Additionally you should ensure any doors are secured on leaving. Taking an extra few moments to follow this checklist could save you a large amount of time going through a security investigation which could result in a monetary penalty or worst case jail time.

Next Slide

Timing	Content	Notes
32 mins		**Slide 18 – Safebase Security Alert System** AC 7.1.2.3

Script for facilitator: (Teaching / learning points)

Safe Base is Defence's security alert system, it communicates the threat of violent acts on defence premises. It is a risk management and response tool underpinned by effective security planning.

The next diagram is a built slide.

There are three threat levels:

Click
AWARE: Security aware - Threat advice indicates a general warning that Defence could be the target of a violent attack. No specific time or location.

Click
ALERT: Increased security - Threat advice of potential attack or act of violence expected in a specific region or specified Defence site, with a specific timeframe.

Click
ACT: Follow emergency procedures - Attack on Defence premises is imminent or underway.

The current Safe Base alert level is displayed every time a person logs onto the DPN and is displayed at both entry and exit points to Defence Sites, including HMAS *Cerberus*.

Each individual defence site will then have instructions that define specific actions for a certain event.

Example 1: An armed intruder has entered the base. The base may be ordered into LOCKDOWN.

Example 2: The OOD has received a telephone call that states 'there are several bombs within the establishment that will detenate in the next 12 hours'. The base may be ordered to EVACUATE.

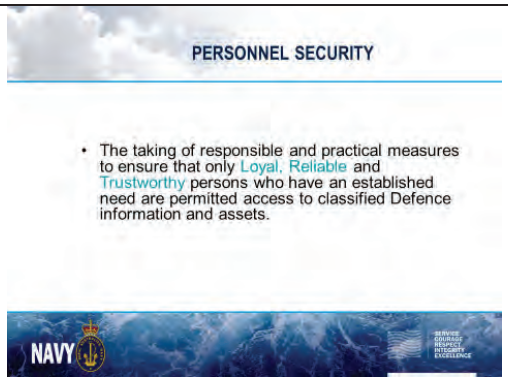
Reiterate that they will hear these instructions every Tuesday when the base alert system is tested.

Next Slide

Timing	Content	Notes
37 mins		**Slide 19 – Personnel Security**

Script for facilitator: (Teaching / learning points)

Personal Security

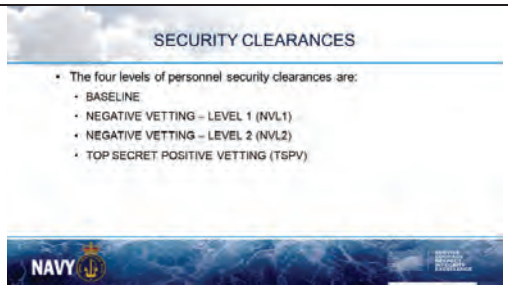
Timing	Content	Notes
37 mins		**Slide 20 – Personnel Security** AC 7.1.3.1

Script for facilitator: (Teaching / learning points)

Read definition from slide.

Definition: Personnel Security is 'The taking of responsible and practical measures to ensure that only Loyal, Reliable and Trustworthy persons who have an established need are permitted access to classified Defence information and assets'.

Next Slide

Timing	Content	Notes
38 mins		**Slide 21 – Security Clearances** No AC

Script for facilitator: (Teaching / learning points)

The four security clearance levels as defined under the PSPF are:

Built Slide

(1) BASELINE: permits access to information or resources up to and including PROTECTED.

CLICK

(2) NEGATIVE VETTING – LEVEL 1 (NVL1): permits ongoing access to information or resources up to and including SECRET.

CLICK

(3) NEGATIVE VETTING – LEVEL 2 (NVL2): permits ongoing access to information or resources up to and including TOP SECRET.

CLICK

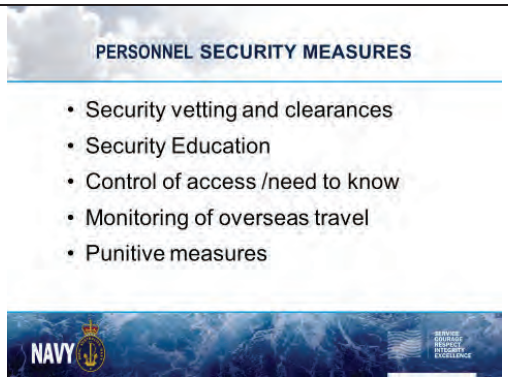
(4) TOP SECRET POSITIVE VETTING (TSPV): permits access to certain types of sensitive, caveated, compartmented and codeword information.

NOTE 1:
To support Defence to appropriately safeguard access to Australian Government resources as a condition of service, new Australian Public Service (APS) employees are to gain and maintain a minimum of a BASELINE security clearance, and Australian Defence Force (ADF) members are to gain and maintain a minimum of an NV1 security clearance.

NOTE 2:
ADF recruits are deemed to hold a BASELINE clearance upon entry to the ADF while their NV1 is assessed. If a recruit is found to be unsuitable to hold an NV1, they may be required to show cause as to why their service should be retained.

Before proceeding to next slide blank current slide and ask students what measures we can take to implement personnel security.

Ask students who may not have contributed to the discussion thus far.

Timing	Content	Notes
43 mins		**Slide 22 – Personnel Security Measures** AC 7.1.3.2

Script for facilitator: (Teaching / learning points)

Next

Security vetting and clearances

Personnel are vetted by the Australian Government Security Vetting Agency before being granted access to classified material. Clearances will only be granted to the required level for a persons role.

Next

Security Education

Throughout your career you will continue to have education on security. This will be via Mandatory Annual Awareness Training (MAAT). Additionally, when entering foreign ports there will be a brief which will include security. Depending on your access level and where you work in the future you will be required to have higher level education and briefings.

Next

Control of access /need to know

Just because you hold a certain security clearance does not mean you can enter any area or access material. Access to areas and material will only be granted to personnel who have a need to know to complete the task.

Next

Monitoring of overseas travel

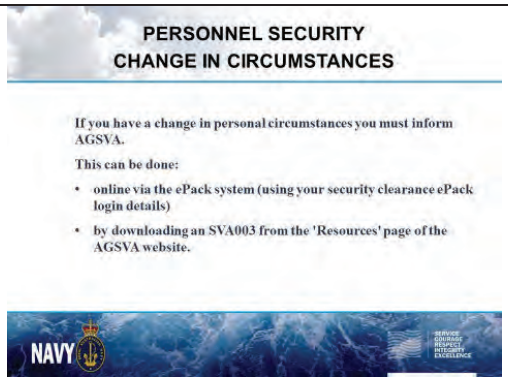
International travel may expose Defence Personnel to threats which could compromise national security. Such threats may not be present in Australia and may therefore not be anticipated by travellers. For this reason it is crucial that travellers are briefed before travel to raise awareness of their destinations security environment ensuring adequate precautions are taken.

Next

Punitive measures

Security incidents are classified as minor or major. The consequences for a deliberate major security incident can be very severe. This could be loss of security clearance, loss of employment or prison time.

Next Slide

Timing	Content	Notes
45 mins		**Slide 23 – Change in Personal Circumstances** AC 7.1.3.3

Script for facilitator: (Teaching / learning points)

If you have a change in personal circumstances you must inform AGSVA.

This can be done:

- online via the ePack system using your security clearance ePack login details or
- by downloading an SVA003 from the 'Resources' page of the AGSVA website.

Next Slide

Timing	Content	Notes
46 mins		**Slide 24 – Change in Personal Circumstances** AC 7.1.3.3

Script for facilitator: (Teaching / learning points)

Built Slide:

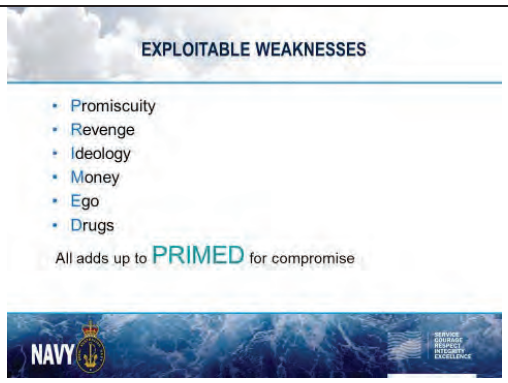
Reporting changes in circumstance helps entities assess personnel security risk based on current and relevant information. Early identification of changes in risk profiles can prevent smaller issues from becoming larger problems. At the individual level, this means encouraging and enabling self-reporting of changes in circumstance by personnel.

QUESTION: What types of circumstances do you think would need to be reported to AGSVA when changed?

- Changes of name/identity (gender)
- Changes in significant relationships
- Changes in share-housing arrangements
- Entering into, or ceasing, a relationship (marriage, civil union or de facto)
- Changes in citizenship or nationality
- Changes in financial circumstances
- Changes in criminal history, police involvement and association with criminal activity
- Involvement or association with any group, society or organisation
- Disciplinary actions
- Drug or alcohol problems
- Residence in, or visits to, foreign countries
- Relatives residing in foreign countries
- Suspicious, persistent or unusual contacts
- Any other significant changes in circumstance.

This list is not exhaustive. If personnel are uncertain whether the information is relevant, report it to the security advisor responsible for personnel security.

Next Slide

Timing	Content	Notes
48 mins		**Slide 25 – Exploitable Weaknesses** AC 7.1.3.4

Script for facilitator: (Teaching / learning points)

Built Slide:

Promiscuity - If a person has frequent sexual activity with different partners or is indiscriminate in the choice of sexual partners their reputation may be open to exploitation. Additionally you may make yourself vulnerable if you cheat on a partner and are keeping this a secret.

Revenge - Revenge could be used against you for many reasons that you have crossed paths with someone that may have something that they can hold against you.

Example: You and your best friend are posted onboard HMAS Collins and are required to conduct a muster of all the classified material for your department. On conducting the muster you discover that you have accidentally destroyed a document with the appropriate witness and procedure. Your friend says don't worry, signs the log to say they witnessed it being destroyed even though they didn't. Does this open you up to revenge later on.

Ideology

Ideology is a collection of ideas or beliefs shared by a group of people. Many political parties base their political action and program on an **ideology**. Your membership of groups may lead you into a position t ochange your beliefs in either the ADF mission or attitude towards security principles.

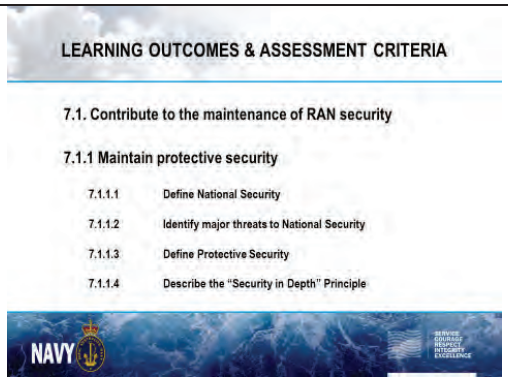
Money - If you place yourself into financial difficulty you obviously open yourself up to exploitation.

Example 1: You are scheduled to deploy to an Area of Operations where your pay will be tax free and you will receive $125 a day extra whilst in the zone. You estimate that during this deployment you will be able to save $60,000 so buy a brand new car worth $70,000 3 months before deploying because you can't wait. 1 month later you injure your knee and are deemed unfit to deploy for 6 months. You are now $70,000 in debt and have now found out that your partner is pregnant.

Ego - An ego is a person's sense of self-esteem or self-importance. Ego becomes an issue when it becomes overpowering. Everyone has an ego, whether big or small.

Drugs – As drugs are an illegal activity in and out of Defence if you are using and haven't been caught you are exploitable by individulas or groups not to report your drug useage/addiction.

This all adds up to **PRIMED** for compromise.

Timing	Content	Notes
50 mins		**Slide 26-28 – LO, SLO and AC**

Script for facilitator: (Teaching / learning points)

Read LO, SLO and AC for entire module.

SLO 7.1.1 Maintain Protective Security
- AC 7.1.1.1 Define national security
- AC 7.1.1.2 Identify major threats to national security
- AC 7.1.1.3 Define Protective Security
- AC 7.1.1.4 Describe the "security in depth" principle

(Next Slide)

SLO 7.1.2 Maintain Physical Security
- AC 7.1.2.1 Define physical security
- AC 7.1.2.2 State measures used to maintain physical security
- AC 7.1.2.3 State the purpose of the SAFEBASE alert system
- AC 7.1.2.4 List close of business routines

(Next Slide)

SLO 7.1.3 Maintain Personnel Security
- AC 7.1.3.1 Define personnel security
- AC 7.1.3.2 List measures used to maintain personnel security
- AC 7.1.3.3 State an individual's responsibilities to maintain personnel security
- AC 7.1.3.4 List exploitable weaknesses in personal character

(Next Slide)

51 mins		**Slide 29 – QUESTIONS** No AC

Script for facilitator: (Teaching / learning points)

Are there any Questions?

Next Slide

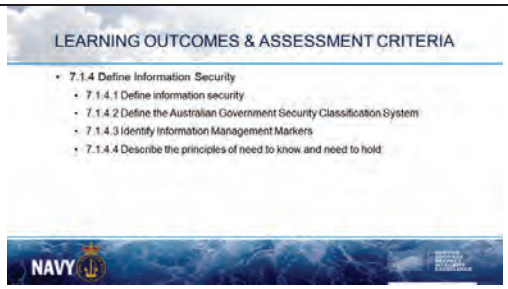
00 mins		**Slide 33 – Security Part Two**

Script for facilitator: (Teaching / learning points)

Welcome class to part two of the security module.

Conduct revision of previous LO's instructed:

Q. Check for knowledge retention of previous lesson through questioning.

3 mins		**Slide 34-36 – Learning Outcomes and Assessment Criteria**

Script for facilitator: (Teaching / learning points)

7.1.4 Define Information Security

7.1.4.1 Define information security

7.1.4.2 Define the Australian Government Security Classification System

7.1.4.3 Identify dissemination limiting markers

7.1.4.4 Describe the principles of need to know and need to hold.

Next

7.1.5 Define Information, Communication and Technology (ICT) Security

7.1.5.1 Define ICT security

7.1.5.2 State measures to maintain ICT Security

Next

7.1.6 Conduct Security Rounds

7.1.6.1 Define the RAN security organisation

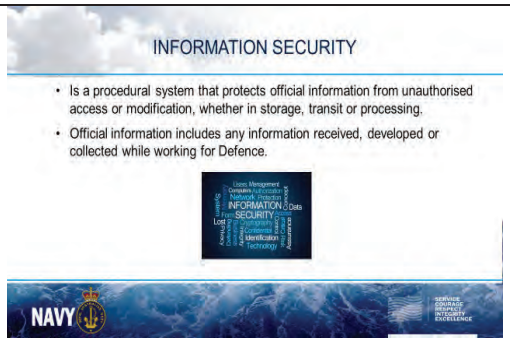
7.1.6.2 Define the role of personnel within the security organisation

7.1.6.3 Identify a security breach

7.1.6.4 Describe the actions to be taken on discovering a security breach

7.1.6.5 Conduct security rounds IAW relevant SSO's

Next Slide

4 mins		**Slide 37 – Information Security** AC 7.1.4.1

Script for facilitator: (Teaching / learning points)

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.

Below not on slide but is to read out

Official Information may include:

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

Information is a valuable resource. Protecting the confidentiality, integrity and availability of information is critical to business operations.

- **Confidentiality** of information refers to the limiting of access to information to authorised persons for approved purposes.
- **Integrity** of information refers to the assurance that information has been created, amended or deleted only by the intended authorised means and is correct and valid.
- **Availability** of information refers to allowing authorised persons to access information for authorised purposes at the time they need to do so.

Next Slide

6 mins		**Slide 38 – Australian Government Security Classifications** AC 7.1.4.2

Script for facilitator: (Teaching / learning points)

There are Six Australian Government Security Classifications:

UNOFFICIAL

OFFICIAL

OFFICIAL: SENSITIVE

PROTECTED

SECRET

TOP SECRET

Next Slide

7 mins		**Slide 39 – Australian Government Security Classifications** AC 7.1.4.2

Script for facilitator: (Teaching / learning points)

Built Slide-Read below first before each classification level.

A classification level is used to indicate the relative importance of classified information to national security and thereby determines the specific security requirements applicable to that information. Clearly defined classification levels are essential to an effective classification system.

The Australian Government Security Classification system has six levels:

Next

Unofficial – For an event such as an Invitation to a Birthday Party.

Next

Official – For information such as Publicly accessible pages on a Defence Website

Next

Official: Sensitive – Procurement details for a defence industry project

Next

Protected – A weapons movement report

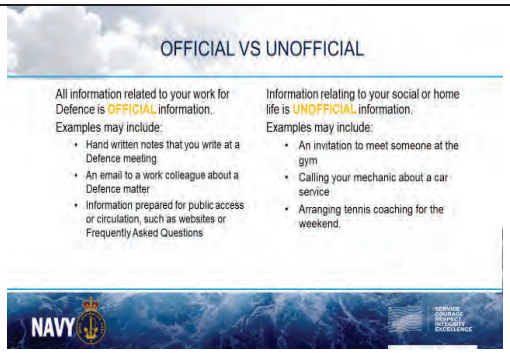
Next

Secret – Operational Military Plans

Next

Top Secret – Intelligence report on a foreign agency

Next Slide

8:30 mins		**Slide 40 – Official Vs Unofficial** No AC

Script for facilitator: (Teaching / learning points)

All information related to your work for Defence is **OFFICIAL** information.

Examples may include:

- hand written notes that you write at a Defence meeting
- an email to a work colleague about a Defence matter
- information prepared for public access or circulation, such as websites or Frequently Asked Questions.

Built Slide – Press for Next Point

Information relating to your social or home life is **UNOFFICIAL** information.

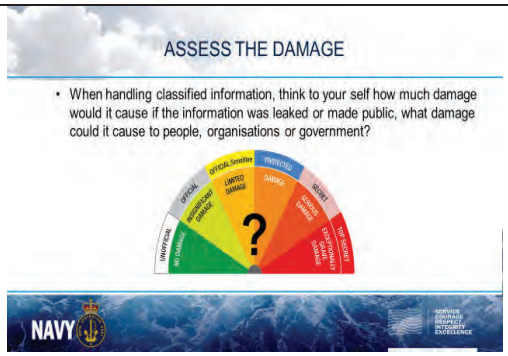
Examples may include:

- an invitation to meet someone at the gym
- calling your mechanic about a car service
- arranging tennis coaching for the weekend.

? What classification would this presentation be?

ANSWER: OFFICIAL

Next Slide

10 mins		**Slide 41 – Assess the Damage** No AC

Script for facilitator: (Teaching / learning points)

When handling classified information, think to yourself how much damage would it cause if the information was leaked or made public, what damage could it cause to **people**, **organisations** or **government**?

Using the slide ask individual students to read out what the damage would be for a certain level.

Unofficial – No Damage

Official – Insignificant Damage

Official: Sensitive – Limited Damage

Protected – Damage

Secret – Serious Damage

Top Secret – Exceptionally Grave Damage

Next Slide

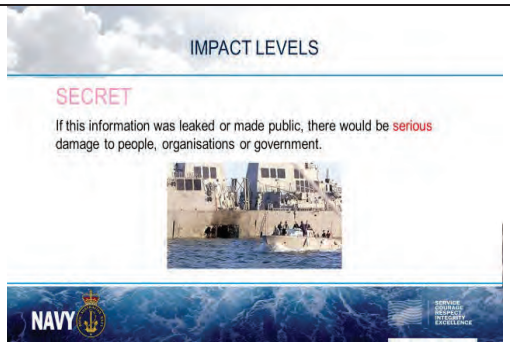
12 mins		**Slide 42 – Impact Levels: Top Secret** No AC

Script for facilitator: (Teaching / learning points)

If Top Secret information was leaked or made public, there would be **exceptionally grave** damage to people, organisations or government. It could cause:

- the collapse of stability in Australia or friendly countries
- the collapse of the Australian economy
- international conflict
- the collapse of all major national infrastructure
- widespread suffering or loss of life.

Next Slide

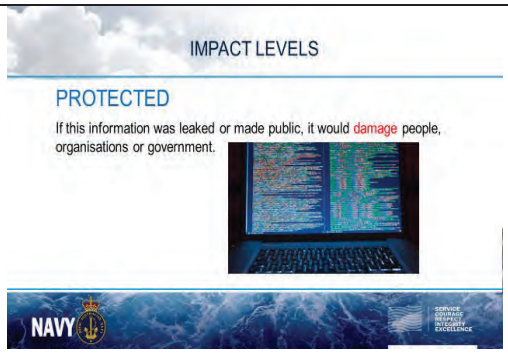
14 mins		**Slide 43 – Impact Levels: Secret** No AC

Script for facilitator: (Teaching / learning points)

- If **Secret** information was leaked or made public, there would be **serious** damage to people, organisations or government. It could cause:

- The internal stability of Australia or other countries
- The operational effectiveness or security of Australian or allied forces
- The continuing effectiveness of highly valuable security or intelligence operations
- Relations with other Governments
- Raise international tensions
- Shut down or substantially disrupt significant national infrastructure

Next Slide

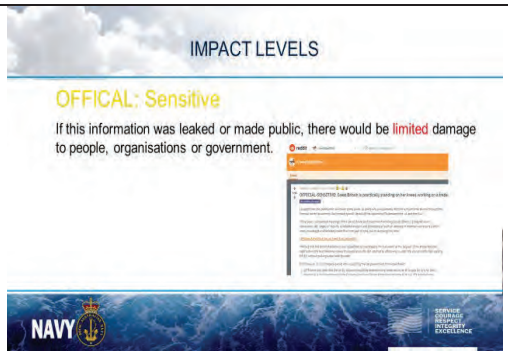
15:30 mins		**Slide 44 – Impact Levels: Protected** No AC

Script for facilitator: (Teaching / learning points)

If **Protected** information was leaked or made public, it would **damage** people, organisations or government. It could cause:

- disruption to one of Defence's main functions
- $100M to $10B damage to Defence assets or budget
- major loss of confidence in government
- suffering or life threatening injury.

Next Slide

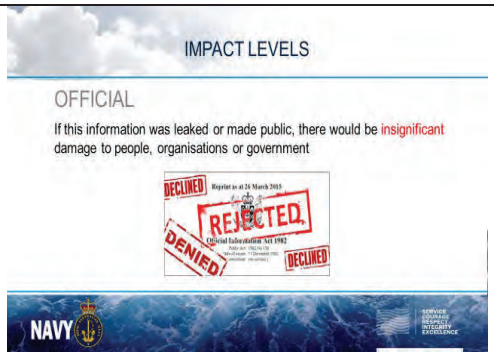
17 mins		**Slide 45 – Impact Levels: Official-Sensitive** No AC

Script for facilitator: (Teaching / learning points)

If **Official: Sensitive** information was leaked or made public, there would be **limited** damage to people, organisations or government. It could cause:

- Defence's business functions to weaken
- $10M to $100M damage to Defence assets
- minor loss of confidence in government
- suffering, harm or injury to someone, but not endanger their life.

Next Slide

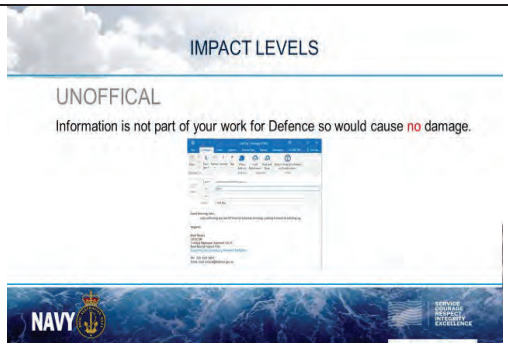
18 mins		**Slide 46 – Impact Levels: Official** No AC

Script for facilitator: (Teaching / learning points)

If **Official** information was leaked or made public, there would be **insignificant** damage to people, organisations or government. It could cause:

- minor issues for routine business operations and diplomatic activities
- minor impact to Defence assets or budget
- no issues with legislation, commercial confidentiality or legal requirements.

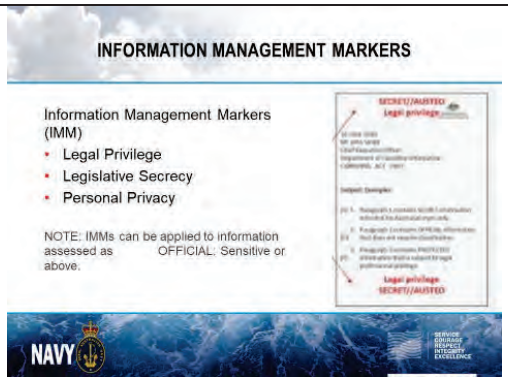
Next Slide

19 mins		**Slide 47 – Impact Levels: Unofficial** No AC

Script for facilitator: (Teaching / learning points)

Unofficial information is not part of your work for Defence so would cause **no** damage.

Next Slide

20 mins		**Slide 48 – Information Management Markers** AC 7.1.4.3

Script for facilitator: (Teaching / learning points)

Built Slide – Next Slide

An Information Management Marker (IMM) is an optional marker that indicates that there are legislative protections for distribution of the information to further restrict information to people with a need to know. It is not a security classification.

Next

- **Legal privilege -** to restrict access and use of information exchange between a lawyer and client for legal advice and proceedings.

Next

- **Legislative secrecy -** to restrict access and use of information where rules for its release are specified in Commonwealth legislation.

Next

- **Personal privacy -** to restrict access and use of personal information that is collected for business purposes as specified under the Pr Privacy Act 1988 (Cth).

Next

IMMs can be applied to information assessed as OFFICIAL: Sensitive or above. IE: Top Secret, Secret, Protected and Official: Sensitive.

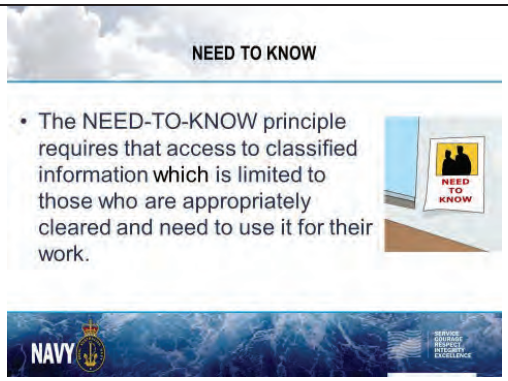
Next

Example of a document which is classified SECRET: Legal Privelege

Blank Slide

Have students open an email and select the security classification of Official. Have them note that they cannot select an IMM. Now have them make an email PROTECTED and note the the IMMs can now be selected.

Next Slide

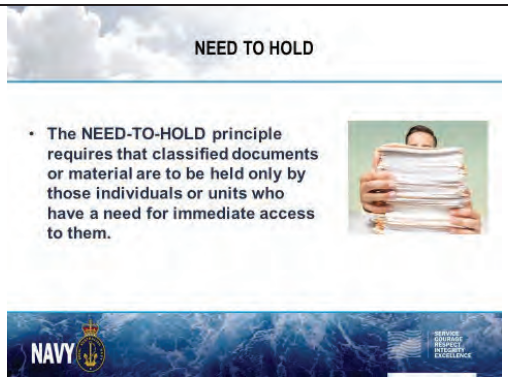
23 mins		**Slide 49 – NEED-TO-KNOW** AC 7.1.4.4

Script for facilitator: (Teaching / learning points)

The NEED-TO-KNOW principle requires that access to the classified information which is limited to those who are appropriately cleared and need to use it for their work.

No one is to have access to classified material just for convenience or a personel interest in a subject to which they are not assigned.

Next Slide

24 mins		**Slide 50 – NEED-TO-HOLD** AC 7.1.4.4

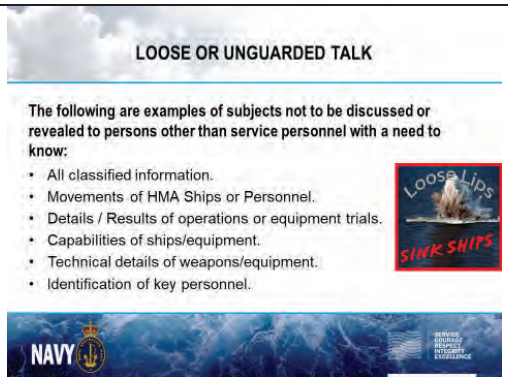
Script for facilitator: (Teaching / learning points)

The **NEED-TO-HOLD** principle requires that classified documents or material are to be held only by those individuals or units who have a need for immediate access to them.

This also ensures units are not holding excessive amounts of classified material if not required to.

EXAMPLE: When the ship enters an extended maintaenence all classified material that is not being used for core business will be returned.

Next Slide

26 mins		**Slide 51 – Loose or Unguarded Talk**

Script for facilitator: (Teaching / learning points)

Regardless of how good our classification system or need to know and hold is, it will not be effective if classified information is discussed in inappropriate locations. Always be mindful of where, who and what is around you.

? Ask class what types of information should not be discussed outside of the workplace?

Remainder on slide built

The following are examples of subjects not to be discussed or revealed to persons other than service personnel with a need to know:

- All classified information

Next

- Movements of Her Majesty's Australian Ships (includes coalition units)

Next

- Details / Results of operations or equipment trial

Next

- Capabilities of ships/equipment

Next

- Technical details of weapons/equipment

Next

- Identification of key personnel

Press for next slide will bring up Loose Lips Sink Ships poster

The slogan **Loose Lips, Sink Ships** originated during World War II to advise service personnel and other citizens to avoid careless talk that might undermine the war effort and is still used today.

Next Slide

29 mins		**Slide 52 – ICT Security**

Script for facilitator: (Teaching / learning points)

The next section will cover Information and Communication Technology Security or, ICT.

Next Slide

29:30 mins		**Slide 53 – ICT Security**

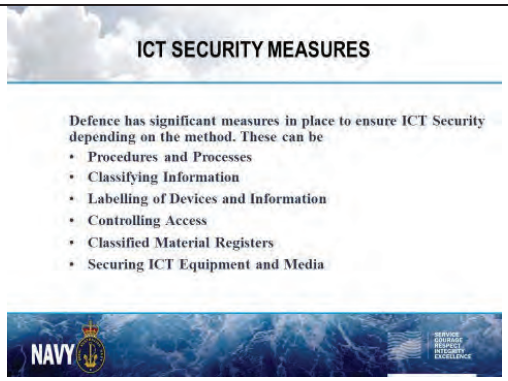
Script for facilitator: (Teaching / learning points)

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

- Computers (including internet and social media)
- Personal Electronic Devices (PEDs)
- Phones
- Multi-Function Devices
- Cyber and Multimedia

Cyber security will be covered in detail at a later date; however, this morning we will specify information that you should be mindful of disclosing.

Next Slide

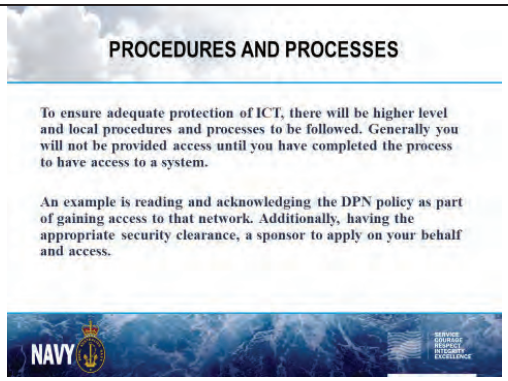
30:30 mins		**Slide 54 – ICT Security Measures**

Script for facilitator: (Teaching / learning points)

Defence has significant measures in place to ensure ICT Security depending on the method. These can be

- Procedures and Processes
- Classifying Information
- Labelling of Devices and Information
- Controlling Access
- Classified Material Registers
- Securing ICT Equipment and Media

Next Slide

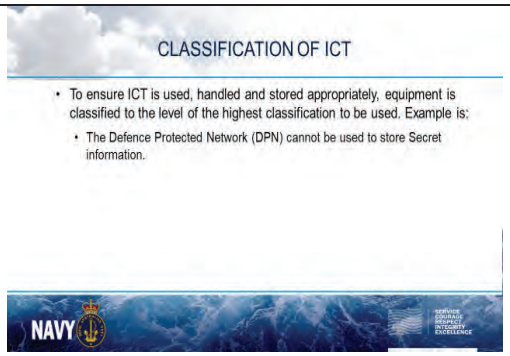
31:30 mins		**Slide 55 – Procedures and Processes**

Script for facilitator: (Teaching / learning points)

To ensure adequate protection of ICT, there will be higher level and local procedures and processes to be followed. Generally you will not be provided access until you have completed the process to have access to a system.

An example is reading and acknowledging the DPN policy as part of gaining access to that network. Additionally, having the appropriate security clearance, a sponsor to apply on your behalf and access.

Next Slide

32 mins		**Slide 56 – Classification of ICT**

Script for facilitator: (Teaching / learning points)

To ensure ICT is used, handled and stored appropriately, equipment is classified to the level of the highest classification to be used.

Built slide

Example 1: The Defence Protected Network (DPN) cannot be used to store Secret information.

Leave Slide Up

QUESTION: You are waiting to have a phone interview for your security clearance from AGSVA. You note that your phone is on low battery and only have your USB cable with you not the wall connection. As you are logged onto the DPN and you consider using it to charge your phone. Will this be a breach of ICT security?

Answer will not display on PPT.

ANSWER: YES your phone is not at required level to plug into a PROTECTED NETWORK.

Next Slide

35 mins		**Slide 57 – Labelling ICT**

Script for facilitator: (Teaching / learning points)

Labelling media Built Slide

Labelling media helps personnel to identify its sensitivity or classification and ensure that appropriate security controls are applied to its handling and usage.
While text-based protective markings are typically used for labelling media, there may be circumstances where colour-based protective markings or other marking schemes need to be used instead. In such cases, the marking scheme will need to be documented and personnel will need to be trained in its use.

To ensure equipment and media are handled correctly they will be clearly labelled. This will include:

Next

Laptops / Tablets – Laptops and Tablets that are classified as Secret or Top Secret will need to be secured in an approved container when not in use.

Next

Hard drives that are part of a network such as the Defence Protected Network and Defence Secret Network do not need to be secured in an approved container when not in use as they utilise a login and password to gain access. They will also be in a building or section that is at the required classification to hold.

Next

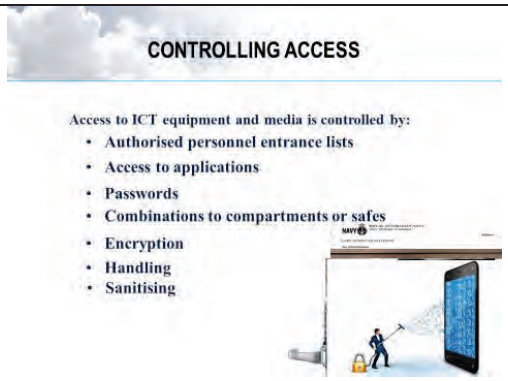
Computer Screens may also have a classification on them or the system that is being used. The classification displayed will be the highest that may be utilised on that system.

Next

USB Drives – When using devices such as USBs particular care needs to be taken when handling mainly due to their size. Whilst small they still need to be labelled.

NOTE: You cannot utilse your own laptop or device for handling classified information.

Next Slide

37 mins		💻 **Slide 58 – Controlling Access**

Access to ICT equipment and media is controlled by:

Built Slide

Authorised Personnel Entrance Lists are used to allow personnel permanent access to compartments. An example would be all CIS sailors accessing the Communication Centre. Personnel not on the list may only enter if approved for a specific duty/time.

Next

Access to applications is controlled to ensure only personnel with a need to access certain applications. An example is the personal details section of the Personal Management Keying Solution (PMKeyS) program. MPO's are approved for access on application due to the nature of their primary role.

Next

Passwords are used to control access to network computers such as the DPN.

You must ensure you lock your workstation when not present. If someone sends an email using your login which discloses protected information to a Foreign Intelligence Service, how will you prove it wasn't you?

Next

Combinations to compartments or safes are used to control access at a higher level. These will normally be used when handling secret or top secret information.

Next

Encryption devices allow information to be passed that is encrypted. Examples are communication circuits from ship to ship.

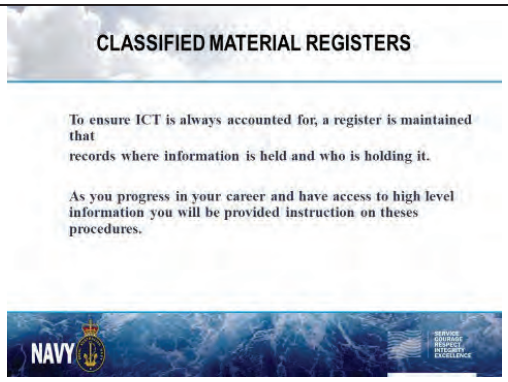
Next

Handling information correctly ensures that it is not left unattended or made available to personnel not cleared for that information.

Next

Sanitising - Routers, switches, network interface cards and firewalls contain memory that is used in their operation. This memory can often retain network configuration information such as passwords, encryption keys and certificates. When disposing of ICT equipment, any media in the ICT equipment should be sanitised in situ or removed and sanitised separately.

Next Slide

39 mins		**Slide 59 – Classified Material Registers**

Script for facilitator: (Teaching / learning points)

To ensure ICT is always accounted for, registers are maintained that records where devices are held and who is holding it.

As you progress in your career and have access to higher level information you will be provided instruction on theses procedures.

NOTE: There must be a trail maintained that can trace each stage of the transfer of the material or device.

Next Slide

40 mins		**Slide 60 – Securing ICT Equipment**

Script for facilitator: (Teaching / learning points)

When ICT equipment is not in use it must be secured in an approved container, vault or compartment.

Below is nice to know:

The pictures displayed are from right to left:

B Class Container for securing secret information

A Class Container for securing Top secret information (normally on shore establishments)

Secure Compartmented Information Facility (SCIF) – is used for CT sailors to man Top Secret networks is used for intelligence team when embarked.

Next Slide

41 mins		**Slide 61 – RAN Security Organisation**

Script for facilitator: (Teaching / learning points)

That completes ICT security, are there any questions on ICT security. We will now go through the RAN Security Organisation.

Next Slide

41 mins		**Slide 62 – RAN Security Organisation**

Script for facilitator: (Teaching / learning points)

Built Slide

Next

The RAN security organisation sits underneath the Chief Security Officer who reports to the Chief of Defence Force and Secretary of Defence.

In accordance with the PSPF, the **Chief Security Officer** is responsible for directing all areas of the Defence enterprise's security to protect Defence's people, information and assets.

Next

The **Director Policing and Security-Navy** (DPS-N) is a Directorate of Navy Headquarters, of the rank of Capatin and is Navy's principal advisor on matters concerning policing and security. Further information on Navy specific security ia aviable at http://drnet/navy/DPSN/Pages/Home.aspx

Next

The **Unit Security Officer** (USO) of each unit will normally be the Execuitve Officer who will appoint an assistant Security Officer for Personal and Physical Security. In Recruit School the Assistant Security Officers are:

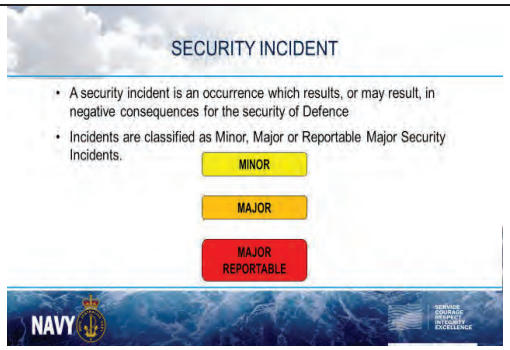
Physical Security: s47E(c) (DO Shipp Division)

Personal Security: s47E(c) (Command Building)

Next

The **Joint Military Policing Unit** (JMPU) is to provide law enforcement on RAN Establishments. The JMPU is a tri-service unit from Navy, Army and Air Force. On HMA Ships the NPC's take on this role. At RAN establishments physical security is supplemented by contracted security firms.

Next Slide

43 mins		**Slide 63 – Security Incident**

Script for facilitator: (Teaching / learning points)

Built Slide

Next

A security incident is an occurrence which results, or may result, in negative consequences for the security of Defence.

Incidents are classified as Minor, Major or Reportable Major Security Incidents.

Next

A Minor security incident is an accidental or unintentional action involving failure to observe protective security policy mandatory requirements or procedures within the Defence Security Principles Framework. Examples include:
Access passes or identification documents lost or left insecure; or security classified material not properly secured or stored.

Next

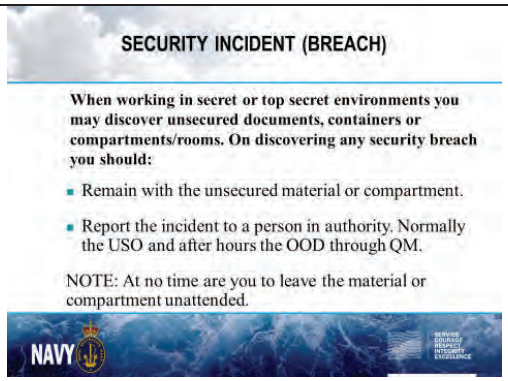
A ***Major*** security incident is any deliberate, negligent or reckless action that leads, or could lead, to the loss, damage, corruption or disclosure of Official Information or assets. Examples include:
a. the loss of material classified 'PROTECTED' or above, or significant quantities of material of a lower Protective Marking;

- Actual or suspected hacking into any information and communications technology (ICT) system;
- Compromise of security keys or combination locks;
- Actual or attempted unauthorised access to an alarm system covering a secured area where security classified information is stored; or
- Repeated incidents involving the same person or work area where the combination of the incidents warrants an investigation.

Next

A ***Reportable Major*** security incident is any occurrence requiring
reporting to the Australian Security Intelligence Organisation (ASIO) as defined I the ASIO Act (1979), including espionage or suspected espionage.
7. An assessment of the harm resulting from a security incident should be used in conjunction with the definitions above to assist in determining whether the incident is a *Minor*, *Major* or *Reportable Major* security incident.

Next Slide

45 mins		**Slide 64 – Learning Outcomes and Assessment Criteria**

Script for facilitator: (Teaching / learning points)

Built Slide

Next

When working in secret or top secret environments you may discover unsecured documents, containers or compartments/rooms. On discovering any security breach you should:

Next

- Remain with the unsecured material or compartment.

On discovering a security incident you should raise the larm whilt remaining with the unsecured material. If a phome is available ring the best POC or use other personnel if available.

Next

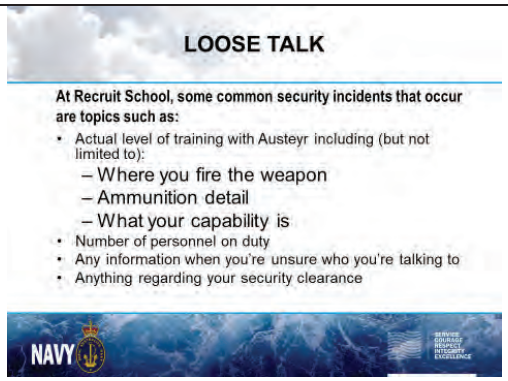
- Report the incident to a person in authority. Normally the USO and after hours the OOD through the QM.

The incident will need to be reported, this is normally done through an immediate supervisor to the USO during working hours. After hours it will need to be reported through dutywatch staff.

Next

NOTE: At no time are you to leave the material or compartment unattended.

Next Slide

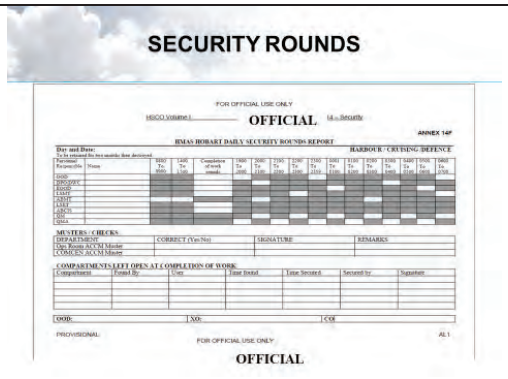
46 mins		**Slide 65 – Learning Outcomes and Assessment Criteria** No AC

Script for facilitator: (Teaching / learning points)

At Recruit School, some common security incidents that occur are topics such as:

- Actual level of training with Austeyr including (but not limited to):
  - Where you fire the weapon
  - Ammunition detail
  - What your capability is
- Number of personnel on duty
- Any information when you're unsure who you're talking to
- Anything regarding your security clearance

Next Slide

47 mins		**Slide 66 – Conduct Security Rounds** AC 7.1.6.5

Script for facilitator: (Teaching / learning points)

As you will note by the Security Rounds sheet displayed almost all members of a dutywatch will have security rounds to conduct.

Allow two minutes for students to review the rounds sheet to see if their individual categories will be part of the rounds routine on HMAS *Hobart*.

? Ask them if they were the ABMT, what times would they be required to conduct rounds.

Answer: 0800, 0900, 2000 and 0200.

Explain from the top each position:

OOD: Rank of LEUT with the watchbill made up form all PQs.

DPO: The Duty Pety Officer is made up of all rates of PO rank with the exception of MT sailors.

EOOD: The Engineering OOD will be a POMT who has gained specific qualifications

LSMT: Made up of LSMT sailors

ABMT: The ABMT position will be an AB or SMNMT.

QM: The QM is a LS of every branch except MT depending on platform.

QMA: The QMA is the same as the QM made up of AB/SMN.

You will note the bottom of the form is then signed on completion of each day by the XO and CO.

You will be taken through the rounds requirements for Recruit School during the round robin on Friday Week One. If this has already been conducted reiterate that they were taken through it.

? Ask if they have any questions.

Next Slide

50 mins		**Slide 67 – Learning Outcomes and Assessment Criteria**

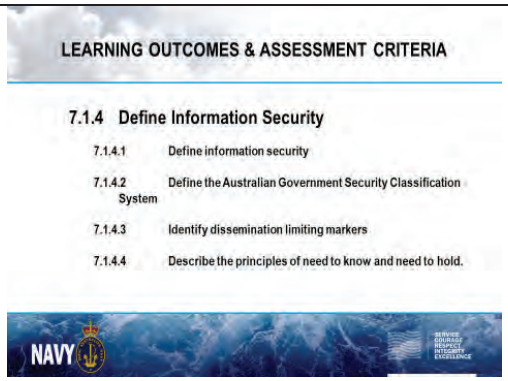
Script for facilitator: (Teaching / learning points)

REMEMBER:

- Security is everyone's responsibility whether on duty or not.
- The picture displayed is of HMAS *Success* that was spray painted when in Wellington, NZ in 2004.

Whilst the crew has painted over half of the message it said “John Howard US Boot Licker”. The perpetrators paddled over on kayaks and could easily have been spotted by a vigilant QM and QMA.

Next Slide

51 mins		**Slide 68-70 – Learning Outcomes and Assessment Criteria** No AC

Script for facilitator: (Teaching / learning points)

7.1.4 Maintain Information Security

7.1.4.1 Define Information Security

7.1.4.2 Identify the Australian Government Security Classification System markings

7.1.4.3 Identify Dissemination Limiting Markers (DLM)

7.1.4.4 Describe the principles of need to know and need to hold

Next

7.1.5. Maintain Information Communication Technology (ICT) Security

7.1.5.1 Define Information Communication Technology Security

7.1.5.2 State measures to maintain ICT security

Next

7.1.6 Respond to a Security Breach

7.1.6.1 Define the RAN security organisation

7.1.6.2 Define the role of personnel within the security organisation

7.1.6.3 Identify a security breach

7.1.6.4 Describe actions to be taken upon discovering a security breach

7.1.6.5 Conduct security rounds IAW relevant SSO's

Next Slide

52 mins		**Slide 72 – Questions** No AC

Script for facilitator: (Teaching / learning points)

Are there any Questions?

Next Slide