Day 3
Questions related to DAY TWO?

Lecture SEVEN
"Ship Security Plan"

SHIP SECURITY PLAN
Purpose Of The SSP

- The SSP is defined in Part A section 2.1.4 of the ISPS Code.
- It is a Plan to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ships stores or the ship from risk of a security incident.

SHIP SECURITY PLAN SUMMARY
Section 9

- The SSP is based on the SSA and therefore is ship specific.
- SSP to be submitted to the flag for approval by the flag administration or RSO.
- Submitted with the SSA, but the SSA is NOT Approved.
- Describes security procedures under different levels of security.
- It is Confidential, must be protected from unauthorised access or disclosure
- It must be retained on board
- Is in the working language of the ship –which if not English, French or Spanish a translation of one of these languages shall be included
- Any amendments must be submitted for approval by the administration before their inclusion.

EU Regulation 725:2004

- REVIEW OF PART B SECTIONS
- 9.2 Minimum Standards for the Ship Security Plan
- 9.4 Independence of RSO's

SHIP SECURITY PLAN – Part A 9.4

The plan shall address, at least, the following:

.1 measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;

.2 identification of the restricted areas and measures for the prevention of unauthorized access to them;

.3 measures for the prevention of unauthorized access to the ship;

.4 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;

.5 procedures for responding to any security instructions Contracting Governments may give at security level 3;

.6 procedures for evacuation in case of security threats or breaches of security;

SHIP SECURITY PLAN Part A 9.4

.7 duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;
.8 procedures for auditing the security activities;
.9 procedures for training, drills and exercises associated with the plan
.10 procedures for interfacing with port facility security activities;
.11 procedures for the periodic review of the plan and for updating;
.12 procedures for reporting security incidents;
.13 identification of the ship security officer;
.

SHIP SECURITY PLAN Part A 9.4

.14 identification of the company security officer including 24-hour contact details;
.15 procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;
.16 frequency for testing or calibration of any security equipment provided on board;
.17 identification of the locations where the ship security alert system activation points are provided; and
.18 procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts

SHIP SECURITY PLAN Part B 9.2

All SSPs should:

.1 detail the organizational structure of security for the ship;
.2 detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;
.3 detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;
.4 detail the basic security measures for security level 1, both operational and physical, that will always be in place;
.5 detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3;
.6 provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances; and
.7 reporting procedures to the appropriate Contracting Governments contact points.

CONFIDENTIALITY ISSUES

- The SSP is confidential and must be protected from unauthorised access or disclosure.
- The SSP in its entirety is not subject to Port State Control inspection - only certain sections may be available in specific circumstances where violations of the Code or SOLAS V and SOLAS XI are apparent .
- Section 9.4 items 2, 4, 5, 7, 15, 17 and 18 cannot be inspected except were agreed between the two contracting Governments
- Some ships may have the plan, misleadingly, split into two parts.

DEVELOPMENT OF THE SSP

- The CSO is responsible for the preparation and submission for approval.
- The SSA is used to prepare the SSP and should be attached to the Plan for approval
- The SSP must be implemented as soon as approval has been given.
- Contracting Government should provide guidance ... as an example
  - The MCA have developed a **Cargo Ship Security Instruction, (CSSI)** which details measures that must be taken into account and measures that must complied with.
  - This allows a consistent application across the UK administrations ships.
- OTHER ADMINISTRATIONS ?????

APPROVAL OF THE SSP

It is the CSO's duty to ensure:

- The SSP is approved by the Administration or an officially appointed RSO.
- The Plan is maintained.
- Should any equipment or measure fail or be suspended this information must be communicated to the Administration / RSO.

B9.4 – EU Reg 725:2004

- All SSP's should be approved by or on behalf of, the Administration.
- If an Administration uses an RSO to review or approve the SSP, that RSO should NOT be associated with any other RSO that prepared or assisted in the preparation of the Plan.

IMPLEMENTATION OF THE SSP

In General

- All Ship personnel must;-
  - Be familiar with and work in accordance with the SSP
  - Understand Procedures at Security Levels 1, 2 & 3.
  - Be aware of the identity of the SSO
  - Undergo Security training, drills and exercises relevant to their responsibilities.

COMMUNICATION & CO-OPERATION BETWEEN SSO, CSO & PFSO

As previously stated;-

The SSO must liaise at the earliest opportunity with the CSO and/or the PFSO regarding:

- Ships arriving in port and pre-arrival requirements.
- Security levels in existence for port/ship.
- An exchange of Relevant security information.
- May include the signing of a Declaration of Security.
- The SSP Must clearly document these communication procedures

MAINTENANCE & MODIFICATION OF THE SSP

- Internal and External Audits
- Continual Review in light of intelligence and operations
- Exercises and debriefing
- Correcting non-conformance reports
- Modifications must be approved and controlled
- Continuous improvement cycle to ensure effectiveness

Developing the Plan

- The SSA will have identified the weaknesses in the systems. It will also have prioritised the risks associated with these weaknesses.
- The development of the plan must address these weakness to mitigate the risk.
- The Plan must consider...

Organisation and Performance of Security Duties

Part B, Section 9.8 THIS IS THE SIGNIFICANT WORKING PART OF THE CODE IN RESPECT OF SHIPS. Addresses measures that could be taken at each security level covering:

.1 access to the ship by ship's personnel, passengers, visitors, etc;
.2 restricted areas on the ship;
.3 handling of cargo;
.4 delivery of ship's stores;
.5 handling unaccompanied baggage; and
.6 monitoring the security of the ship.

ACCESS CONTROL

- 9.9 The SSP should establish the security measures covering all means of access to the ship identified in the SSA. This should include any:

.1 access ladders;
.2 access gangways;
.3 access ramps;
.4 access doors, side scuttles, windows and ports;
.5 mooring lines and anchor chains; and
.6 cranes and hoisting gear.

ACCESS POINTS

9.14 Part B

(Items for Consideration)

- ID Checks
- Secure Search Areas
- Vehicle Searching
- Segregation of Search and non Searched Persons & Embarking/disembarking passengers
- Visitor Escorts
- Access for stevedores
- Staff Security Threat briefings

TYPICAL RESTRICTED AREAS

- The Bridge (including monkey island)
- Communication, Security and Surveillance spaces. Lighting Controls.
- Machinery Spaces and Control Stations
- Cargo Pump and control rooms
- Cargo Spaces and Stores rooms
- Emergency generator and battery rooms
- Fan / ventilation spaces
- Fire stations
- Store rooms for dangerous goods
- Potable water Tanks and Pumps
- Crew accommodation
- ALL Vulnerable areas identified in the SSA

RA's & REQUIRED LAW

The UK Position as an example
SI1495:2004 as amended

- RA defined in relevant legislation
- The law requires an RA to provide for;
  - Clear identification within the Plan
  - Notices/Signs which can clearly be seen by persons entering the RA
  - Entry by a person only with permission, conditional or otherwise.
  - These requirements are generally met by Physical Security (fences, gates), supervision and a Pass system
- MALTA has similar provisions on ports in **S.L.352.21**

RESTRICTED AREAS

9.18 Part B

(Items for Consideration)

- Staffed at all times?
- Man, Lock or tag access points?
- Utilise surveillance equipment as appropriate?
- PTZ CCTV Systems Deployed?
- Frequent and irregular patrols?
- Intrusion detection alarms?

HANDLING CARGO

Sec 9.25 Part B
(Items for consideration)

- Prevent cargo that is not intended for carriage aboard from being accepted and stored onboard the ship
- Prevent tampering of the cargo
- Prevent stowaways and unauthorised persons from boarding
- At Level 3 – Sec 9.32.1 Part B
  - Suspension of loading and unloading of Cargo

VIGILANCE !

HANDLING STORES
9.33 Part B
(Items for consideration)

- Check integrity of all packaging
- Inspect all items before accepting
- Adopt measures to Prevent tampering
- Don't accept any items unless absolutely certain they are for the ship
- At Level 3 – Sec 9.17.5 Part B
  - Extensive Checking
  - Suspension of Handlings Ships Stores
  - Refusal to Accept Ships Stores.

VIGILANCE !

UNACCOMPANIED BAGGAGE
9.38 Part B
(Items for Consideration)

- Procedures for Screening and Searching Unaccompanied baggage must be in place relative to the Specific Security Level
- Unaccompanied Crew baggage should be subjected to the same levels of scrutiny.
- Where the port facility and the ship have suitable equipment for screening, responsibility for screening rests with the Port.
- There should be close co-operation between the ship and the port facility in this regard

VIGILANCE !

MONITORING SHIP SECURITY
9.42 Part B
(Items for Consideration)

- Lighting Provision
- Adequately trained and motivated watchkeepers, security staff and watches.
- Adequate and non scheduled Patrolling
- Use of Intrusion Detection and surveillance devices
- Requirements to monitor the area around the ship

VIGILANCE !

Ship-Ship Interface

- Same measures apply
- Responsibility to vessel to ensure compliance

Questions?

COFFEE

Lecture EIGHT
"ISPS AND ISM"

Safety versus Security

- Sometimes Conflicts

ISM CODE & ISPS CODE

INTERNATIONAL MANAGEMENT SAFETY CODE

- Initially came into force 1st July, 1998 but origins go back into the 1980's
- Revised Guideline – 2002
- Further amendments with the current edition from 1st July, 2010

INTERNATIONAL SHIP & PORT FACILITY SECURITY CODE & SOLAS Amendments 2003

SIMILARITIES AND RELATIONSHIPS BETWEEN SAFETY AND SECURITY

ISM

- 1994 Amendments to SOLAS 1974 Convention entered into force on 1st July, 1998
- Introduced a new Chapter IX – ISM Code
- Mandatory
- Origins in 1980 – came out of increased concern of poor management standards
- 'HERALD OF FREE ENTERPRISE'
- Provides guidelines on Management for the safe operation of, and pollution prevention from, ships
- Chapter IX amended by resolution MSC.99(73) and accepted on 1st January 2002.
- Resolution MSC.194(80) came into force on 1st January 2009 leading to the Current 2010 edition of the code.

2010 Edition

Incorporates a number of changes/additions

- 1.1.10 Revised definition of Major non-conformity
- 1.2.2 Need for Risk Assessment methodology
- 5.1.5 Periodical review by Master
- 7 'Shipboard Operations' intent clarified
- 9.2 Preventative actions introduced
- 10.3 Critical standby systems intent clarified
- 12.1 Internal Audit 12 month max requirement
- 12.2 Company to periodically review SMS effectiveness
- 13.12 Renewal Audits after expiry of Certificate
- 13.14 Extension of SMC for vessel to complete voyage
- 14.4.3 Internal Audits completed within 3 months of interim Audit

ISPS

- In force?
- Which Chapter of SOLAS?

ISM REGULATION 2

- Application - Applies to all ships regardless of date of construction;
- Passenger ships including High speed craft, not later than 1st July, 1998
- Oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed craft of 500 gross tonnage and upwards, not later than 1 July 1998
- Other cargo ships and mobile offshore drilling units of 500 gross tonnage and upwards, not later than 1 July, 2002

Does not apply to Government-operated ships used for non-commercial purposes

ISPS REGULATION 2

- ISPS Code applies to
- ?
- ?
- ?
- ?

3.3 The Code does not apply to warships, naval auxiliaries or other ships owned or operated by a contracting government and used only on government non-commercial service

ISM – Regulations 3 & 4

- 3.1 The company and ship shall comply with the requirements of the ISM Code. For the purpose of this regulation, the requirements of the code shall be treated as mandatory.
- 3.2 The ship shall be operated by a company holding a Document of Compliance.

- 4.1 DoC issued to every company which complies with requirements of the ISM Code. Issued by the Administration or by an organisation recognised by the administration, or at the request of the administration another Contracting Governments

ISPS Regulation 3, 4 and 5

- 3. Obligations of Contracting Governments
- 4. Requirements for Companies and Ships of the Company ?
- 5. Specific Responsibility of Companies

- Is the ISPS Code mandatory?
- Who ensures the ship complies with the ISPS Code?
- Is the Company Security Policy approved?

ISM Regulation 6

- Verification & Control

- 6.1 The Administration, another Contracting Government at the request of the administration or an organisation recognised by the Administration shall periodically verify the proper functioning of the ships Safety Management System
- A Ship shall hold a certificate issued pursuant to the provisions of regulation 4.3 shall be subject to control in accordance with the provisions of regulation XI/4

SOLAS XI-2 Regulation 9 and ISPS A19

- Control and Compliance
- 19.1.4 The security system and any associated security equipment of the ship after verification shall be maintained to conform with the provisions of regulations XI-2/4.2 and XI-2/6, this part of the Code and the approved ship security plan. After any verification under section 19.1.1 has been completed, no changes shall be made in security system and in any associated security equipment or the approved ship security plan without the sanction of the Administration.
- 19.2 Issue or endorsement of certificate
  - 19.2.1 An International Ship Security Certificate shall be issued after the initial or renewal verification in accordance with the provisions of section 19.1.

Company Responsibilities & Authority/Obligations

ISM 3.
- Who has Responsibility for the ship
- Document the responsibility
- Provide adequate resources and shore based support

ISM 4 & 5
- Designated Person
- Masters Responsibility and Authority

ISPS 6.
- SSP Statement of Masters Authority
- Support CSO, SSO and Master

5. ISM MASTERS RESPONSIBILITY & AUTHORITY

- Company to define Master's responsibility in regard to;
  - Implementing safety & environmental company policy
  - Motivating Crew
  - Issuing orders and instructions in clear simple manner
  - Verify specified requirements are observed
  - Review the SMS and report deficiencies to shore management

ISPS OBLIGATIONS OF THE COMPANY

- 6.1 The Company shall ensure that the ship security plan contains a clear statement emphasizing the master's authority. The Company shall establish in the ship security plan that the master has the overriding authority and responsibility to make decisions with respect to the security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary.
- 6.2 The Company shall ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfil their duties and responsibilities in accordance with chapter XI-2 and this part of the Code.

- SOLAS XI-2 Reg. 8

Resources and Personnel

- ISM 6.
- 6.4 All personnel involved in SMS to have adequate understanding of rules, regulations, codes and guidelines

- ISPS B13.4
- All other shipboard personnel should have sufficient knowledge of and be familiar with relevant provisions of the SSP, including:
  - .1 the meaning and the consequential requirements of the different security levels; .....

Development of Plans

- ISM 7 -The Company should establish procedures for the preparation of plans and instructions, including checklists as appropriate, for key shipboard operations concerning the safety of the ship and the prevention of pollution. The various tasks involved should be defined and assigned to qualified personnel
- ISPS A9.1 - Each ship shall carry on board a ship security plan approved by the Administration. The plan shall make provisions for the three security levels as defined in this part of the Code.

ISM 10 – Maintenance of the Ship

- Inspections
- Report non-conformities
- Take corrective actions
- Record the activities

ISM 11 - Documentation

- Valid documents available at all relevant locations
- Changes to documents are reviewed and approved by authorised personnel
- Obsolete documents are promptly removed

ISPS A9 & A10

- 9.6 The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorised deletion, destruction or amendment.
- 9.7 The plan shall be protected from unauthorized access or disclosure.

- 10.1 Records of the following activities addressed in the ship security plan shall be kept on board for at least the minimum period specified by the Administration, bearing in mind the provisions of regulation XI- 2/9.2.3:
- 10.3 The records may be kept in an electronic format. In such a case, they shall be protected by procedures aimed at preventing their unauthorised deletion, destruction or amendment.

ISM 12 – Company verification, Review and Evaluation

- Internal Safety Audits
- Efficiency of SMS
- Audits with corrective actions and in accordance with documented procedures
- Personnel carrying out Audits should be independent of area audited
- Unlike ISM, ISPS has included provided the Contracting Governments not only with initial renewal verifications, but with the provision for additional verifications as necessary – ISPS A19.1.1.4

ISPS

- A9.4 The plan shall address, at least, the following:
  - 8. procedures for auditing the security activities;
  - 9. procedures for training, drills and exercises associated with the plan;
  - 11. procedures for the periodic review of the plan and for updating;
- 9.4.1 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship.

SUMMARY

- Many similarities between ISM & ISPS
- Clear Link between Safety and Security
- SOLAS XI-Regulation 8. Masters Responsibility. Safety takes precedence over Security
- Control and compliance measures are more rigorous in respect of ISM.
- The DAO's powers are more restricted in respect of ISPS

QUESTIONS?

EXERCISE 3
ACCESS - SUCCESS

LUNCH

Lecture NINE

PORT SECURITY ASSESSMENT AND PLANNING

Brief Overview

What is a port facility security assessment (PFSA)?

The PFSA process is a process by which competent persons identify key assets within a port facility, assess the threats to these assets and identify security measures that can be implemented to reduce the vulnerability of these assets.

THE FIRST STAGE OF COMPLYING WITH ISPS REQUIREMENTS

PROCESS
ISPS Code A 15.5

- The PFSA shall include at least the following elements
  - Identification and evaluation of important assets and infrastructure it is important to protect. (B15.3 and B15.7)
  - Identification of possible threats to assets and infrastructure and the likelihood of their occurrence, in order to prioritise security measures (B 15.11)
  - Identification, selection and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability (B15.14)
  - Identification of vulnerability, including human factors, in the infrastructure, policies and procedures (B 15.5)

PORT FACILITY ASSESSMENT
Code B 15.3

- Generic Assets which require protection
- Physical Security
- Structural Integrity
- Personnel protection systems
- Procedural Policies
- Radio and Telecommunication systems including computer systems and networks
- Relevant transportation infrastructure
- Utilities
- Other areas which may, if damaged or used for illicit observation pose a risk to persons, property, or operations within the port facilities

PORT FACILITY ASSESSMENT
Code B 15.7

- Specific assets which require protection:
- Access, entrances, approaches and anchorages, manoeuvring and berthing areas
- Cargo facilities, terminals, storage areas, and cargo handling equipment
- Systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks
- Port vessels traffic management systems and aids to navigation
- Power plants, cargo transfer piping and water supplies
- Bridges, railways, roads

PORT FACILITY SECURITY ASSESSMENT
Code B 15.14

- Security measures should be selected on the basis of factors such as whether they reduce the probability of an attack and should be evaluated using information that includes:
- Security surveys, inspections and audits;
- Consultation with port facility owners and operators, and owners/operators of
- Adjacent structures if appropriate;
- Historical information on security incidents; and
- Operations within the port facility.

PORT SECURITY ASSESSMENT
EU Directive 65:2005

- Implemented by 15 June 2007.
- PSA Should address
  - Areas relevant to **PORT** Security thus also defining the Port boundaries.
  - Identify security issues deriving from interface between Port and Port facility and other Port security measures.
  - Identify Port personnel who will be subject to background checks/security vetting because of involvement in high risk areas
  - Identify risk variations based on seasonality
  - Identify possibility of Cluster effects on Security incidents
  - Identify need to know requirements of all those directly involved as well as the general public

BS ISO 20858:2007

- **Voluntary process with Certification if followed and evidenced.**
- **Provides guidance for persons carrying out the Assessment process.**
- **Does not affect the requirements of Contracting Government.**
- **Provides common International Standard to the process for all ports participating.**

The UK Position
TRANSEC PROTECTION CATEGORIES

EU Dir 65:2005 – UK has Subdivided the Port according to likelihood of the risk of a security incident

PAX - International Passenger Ships; Domestic AMSA/TRANSEC Operations

COG - Chemical, Oil, Gas

CRR - International Containers & Ro-Ro traffic

OBC - International Other Bulk Cargo

Other EC Member States

?

TRANSEC CATEGORIES OF PORT FACILITIES

PAX,COG,CRR,OBC require a PFSO & a PFSP, including Contingency Plans

PAX, COG & CRR:- (Restricted Areas) enforced at all levels

OBC Enforced at Levels 2 & 3

Other ports Security contact nomination only

PFSP -Purpose of the PFSP

- The PFSP is defined in Part A Section 2.1 of the ISPS Code and is to ensure the application of measures to protect the Port facility from risks of security incident.
- The PFSO is responsible for the development, implementation, revision and maintenance of the PFSP and for liason with the SSO or CSO.
- The PFSP must address the measures taken at the three security levels;

Port Facility Security Instruction (PFSI)

- Following the PFSA, TRANSEC provides a Report and a PFSI(s) for the Port Categorisation.
- The purpose of the PFSI is to provide detailed Instruction and guidance on implementing the required Security measures, preparation of the PFSP and completion of the PFSP Template.
- PFSI's contain detailed information on Security measures in Ports and are RESTRICTED documents.

Port Facility Security Plan Template

- Also in order to assist UK PFSO's in ensuring the PFSP meets the legal requirements a Port Facility Security Plan Template has been developed by TRANSEC.
- It is used by ALL UK Port facilities when drawing up their plans
- What is the position in other EC member states???

PFSP - Contents Section 16 Parts A&B

- A Port Facility Security Plan will be developed and maintained on the basis of a Port facility Security Assessment for each Port Facility
- The plan shall make provision for the three security levels
- The plan shall be in the working language of the Port
- The plan shall be approved by the contracting government
- The plan may be part of other emergency plans
- The plan shall be protected from unauthorised access or disclosure

PFSP – Part A 16.3

The plan shall address :-

- Prevention of weapons or other dangerous substances and devices from being introduced into the port or aboard ship
- Prevent unauthorised access to the port facility or ships
- Procedures for responding to security threats or breaches of security
- Procedures for responding to security instructions from the contracting government
- Procedures for evacuation
- Duties of port facility personnel assigned to security responsibilities

PFSP – Part A 16.3

- Procedures for interfacing with ship security activities
- Procedures for periodic reviews of the plan
- Procedures for reporting security incidents
- Identification of the PFSO including 24 hour contact
- Measures to ensure the security of information in the plan
- Measure to ensure the effective security of cargo and cargo handling equipment in the port
- Procedures for auditing of the plan
- Procedures for responding to a security alert system of a ship at the port
- Procedures for facilitating shore leave for ship's personnel and allowing access of visitors to ships

16.9 Implementing the PFSP

- Access to Port Facility
- Restricted area within Port facility
- Handling Cargo
- Delivery of Ships Stores
- Handling unaccompanied baggage
- Monitoring the Security of the Port facility

Designated Temporary Restricted Areas (TRA)

- Requirements to designate TRA's will be determined in the PFSA
- Based on type of traffic normally handled by the Port facility and the potential for the specific types of traffic and cargo to be handled. (Cruise ships, Military vessels and dangerous goods).
- Before bringing a TRA into use, a thorough sweep of the area must be carried out. (16.21 B)
- They must be secured, monitored and search regimes implemented in line with those of Permanent RA's

CONFIDENTIALITY ISSUES

16.8 The PFSP is confidential and must be protected from unauthorised access or disclosure as identified in previous slides.

However.....

18.3 All Port Facility personnel should have knowledge of and be familiar with relevant provisions of the PFSP in...

18.3.1 The meaning and consequential requirements of the different security levels

PENALTIES

- In U.K. under the Ship and Port Facility (Security) Regulations 2004, Failure to comply with the requirements detailed in SI1495 can result in an Enforcement Notice being served on the PFSO.
  - Failure to conform to such Notice may result in Court appearance and Fine. Continued failure after conviction can result in £100 per day fine until conforming to the Enforcement Notice.
- Eire – SI413 – Offences fine of €3000

Questions?

Lecture TEN
"Security Responsibilities"

ISPS CODE RESPONSIBILITIES 1

CONTRACTING GOVERNMENTS

SET SECURITY LEVELS AND PROVIDE GUIDANCE FOR PROTECTION FROM SECURITY THREATS.
REVIEW, APPROVE, VERIFY and CERTIFY PFSP's and SSP's

EU725:2004 Para 13. Requires Member States to authorise a competent body to carry out security checks as per Council Directive 21/1995

EU Regulation 324/2008 lays down procedures for Commission inspections for Imaritime Security

ASIDE

- *EC468/1999 Lays down procedures for the exercise of implementing powers conferred on the commission.*
- *Standardisation of implementation without creating unfair competition across EC*

Setting the Level
Part A Sect 4.1

.1 The degree that the threat information is credible;
.2 The degree that the threat information is corroborated;
.3 The degree that the threat information is specific or imminent; and
.4 The potential consequences of such a security incident.

IMO - MSC 1132 Refers

IMO - MSC 1132.
Para 3

Administrations have to ensure that security level information is provided to ships entitled to fly their flag and Contracting Governments have to ensure that security-level information is provided to port facilities located within their territory and to ships prior to entering a port and when in a port within their territory. Security-level information has to be updated as circumstances dictate.

CONTRACTING GOVERNMENTS

Ensure appropriate measures are in place to avoid unauthorized disclosure or access to:

- Ship Security Assessments
- Ship Security Plans
- Port Facility Security Assessments
- Port Facility Security Plans

European Union Position

EC Regulation No 725/2004

- EU Regulation on enhancing ship and port facility security provides for consistent implementation of the IMO requirements across Europe.
- As we have seen, the Regulation makes selected paragraphs of Part B of the ISPS Code (the guidance section) become mandatory for Member States
- The Regulation also extends the scope of the IMO requirements to Class A domestic passenger ships and the port facilities that serve them and to other domestic operations on the basis of risk assessment which the member states are required to undertake.

LEGAL FRAMEWORK

- As previously discussed....
- Regulation (EC) No 725/2004 on enhancing ship and port facility security, which came into force on 19 May 2004, gives direct legal effect to the ISPS Code in the E.U.
- In the UK this Regulation is accompanied by the Ship and Port Facility (Security) Regulations 2004 SI 1495 - which put in place an enforcement and compliance regime for the UK. These Regulations came into force on 1 July 2004
- Member States will have appropriate legislation in place to provide for this implementation.
- Directive (EC) N0. 65/2005 on enhancing Port Security Entered into force on 15th June, 2007 this requires EU Member States to consider all aspects of a PORTS Operation in respect of security.

Port State Control

REGULATION XI -2/9

- Control & Compliance For the purpose.....
  - WHAT DOES THIS MEAN TO YOU?
  - Legal provision for each Member State?
  - What is yours, i.e UK,Ireland Statutory Instruments , Malta SL, France Decree, Germany Protocol.

EU725:2004

- REQUIRES MEMBER STATES TO.....
- Preamble
  - Para 11. Vigorously Monitor Compliance.
  - Para 13. May Undertake Security Checks for enforcement
  - Para 16. Implement Powers conferred by Commission
- Article 6
  - Requirement for Member States to ensure that special measures to enhance Maritime Security are applied by ships on entry to Port.
  - Para 2.1 – Regulation 9 – Pre Arrival information
- Article 8
  - Security Checks – Certificate verification
- Article 9
  - Implementation and conformity Checking

MSC 1111:2004

- Para 1.6 Describes Control and Compliance measures applicable to ships to which SOLAS XI-2 applies and divides into three sections the requirements of these Control & Compliance Measures
  - Control of ships already in Port
  - Control of Ships intending to enter a Port of another Contracting Government
  - Additional Provisions applicable to both salutations (ISPS Code Para B4.29)

OFFENCES - HOW ARE REQUIREMENTS ENFORCED?

- Ship and Port Facility (Security) Regulations 2004 – Related to Unauthorised entry to Restricted Areas on Ships and Port Facilities, and removal from same and obstructing authorised persons in execution of duties. Summary Offence £5,000 fine
- Public Order Act 1984 – To substitute for offence's removed as result of application of AMSA on ports.
- Maritime Security compliance enforcement – Deficiency Notices (DN) – No penalty, but failure to implement/rectify will result in the issuance of an Enforcement Notice (EN). Failure to comply with an EN is an offence and carries legal penalty

RECOGNISED SECURITY ORGANISATION (RSO)

- Must have proven expertise in the security field to have "Recognised" status.
- Authorised by Contracting Governments to:
  - Approve SSPs or amendments on behalf of Contracting Government for ***Ships of their Flag***
  - Verify and certify compliance of ships
  - Conduct Port Facility assessments

MSC/Circ.1074 10 June 2003

- **MEASURES TO ENHANCE MARITIME SECURITY**
- **INTERIM GUIDELINES FOR THE AUTHORIZATION OF RECOGNIZED SECURITY ORGANIZATIONS ACTING ON BEHALF OF THE ADMINISTRATION AND/OR DESIGNATED AUTHORITY OF A CONTRACTING GOVERNMENT**

ASSIGNMENT OF R.S.O's -1

- Where a Contracting Government chooses to authorise an RSO to act on its behalf they must first:

  B 4.5
  - Ascertain their experience in aspects of Security
  - Verify their knowledge of Ship and Port Operations
  - Identify their capability to assess likely Security Risks
  - Assess their ability to maintain and improve the expertise of their staff

ASSIGNMENT OF R.S.O's - 2

- Maintain trustworthiness of personnel
- Adopt measures to avoid unauthorised disclosure of Security related information
- Have a knowledge of Ch. XI-2 and Part A of the Code and any pertinent legislation
- Knowledge of current Security Threat or pattern's
- Recognition of weapons and dangerous substances

ASSIGNMENT OF R.S.O's - 3

- Knowledge of Characteristics and Behavioural patterns of those likely to threaten security
- A knowledge of techniques used to circumvent security measures
- A knowledge of Security Surveillance Equipment and operational limitations

ENGAGEMENT OF RSO's

- So when delegating RSO's to carry out work for them Contracting governments should ensure that the RSO has the competencies to undertake the task. Verification procedures must therefore be in place
- A Port or Harbour Authority or Port Facility Operator may be appointed as an RSO provided it has the necessary security related experience.

WHAT AN RSO CANNOT DO!!

- Sec A 4.3
  - Set the Security Level
  - Approve the PFSA and amendments
  - Determine the Port Facilities which have a PFSO
  - Approve the PFSP
  - Exercise Control and Compliance measures pursuant to Regulation XI - 2/9

ISPS CODE RESPONSIBILITIES 2

SHIPPING COMPANIES

IMPLEMENT and MAINTAIN THE SSP VIA REVIEW & AUDIT.
APPOINT and SUPPORT THE CSO, SSO and MASTER

THE COMPANY (Shipping)

Sect 2.1.8 Part A

- Must provide the Master with information pertaining to:
  - Persons responsible for appointing shipboard personnel
  - Parties responsible for deciding the employment of the ship.
  - Contact details of Time or Voyage and Charterer's

COMPANY SECURITY OFFICER

Part A - 11.2

THE CSO DUTIES WILL INCLUDE :-

- advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;
- ensuring that ship security assessments are carried out;
- ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;
- ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;
- arranging for internal audits and reviews of security activities;
- arranging for the initial and subsequent verifications of the ship by the Administration or the RSO;

COMPANY SECURITY OFFICER

Part A - 11.2

- ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;
- enhancing security awareness and vigilance;
- ensuring adequate training for personnel responsible for the security of the ship;
- ensuring effective communication and co-operation between the SSO and the relevant PFSO's;
- ensuring consistency between security requirements and safety requirements;
- ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and
- ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

ISPS SOLAS Requirements

REQUIREMENTS FOR SHIPS ARE AS WE HAVE SEEN;

- Fitting of an Automatic Identification System
- Fitting of a Ship Security Alert System
- Provision of a Continuous Synopsis Record
- Marking the Vessel with an Security Identification Number
- Maintain a CSR

SHIP SECURITY OFFICER

Part A 12.2

- THE SSO IS ACCOUNTABLE TO THE MASTER FOR HIS DUTIES. DUTIES INCLUDE BUT ARE NOT LIMITED TO:
  - Undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;
  - Maintaining and supervising the implementation of the SSP including any amendments to the plan;
  - Co-ordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant PFSO;
  - Proposing modifications to the SSP;

SHIP SECURITY OFFICER

Part A - 12.2

- Reporting to CSO any deficiencies and non-conformities identified during internal audits, carrying out periodic reviews, security inspections and verifications of compliance and implementing any corrective actions:
- Enhancing security awareness and vigilance on board;
- Ensuring that adequate training has been provided to shipboard personnel, as appropriate;
- Reporting all security incidents;
- Co-ordinating implementation of the SSP with the CSO and the relevant PFSO;
- Ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

PORT FACILITY SECURITY OFFICER

Part A – 17.2

- Conducts initial survey; develops, implements, maintains and Exercises the Port Facility Security Plan
- Undertakes regular security inspections
- Recommends modifications and corrects deficiencies in the PFSP.
- Enhances security awareness in staff
- Ensures adequate training is provided for Port Facility personnel

PORT FACILITY SECURITY OFFICER

Part A – 17.2

- Keeps records; reports incidents
- Coordinates the plan with CSOs/SSOs/Security Services
- Assists SSO's in confirming the identity of those wishing to board
- Ensures standards of personnel, equipment and it's maintenance
- Completes a Declaration of Security when required.

Questions?

COFFEE

LECTURE 11
ASSESSMENT AND REVIEW

MONITORING & CONTROL

- It is essential that **SSP is** reviewed regularly deficiencies and non conformances noted and improvements implemented

Recall that

- All Amendments/improvements identified must be submitted to the Contracting Govt for approval before their implementation

Review Requirements

- Internal review required by the Company
- External Review Required by the Administration (Verification)

EC 324/2008
Article 2

- Provides some useful definitions in regards to Commission Inspections.
- These can be considered in general terms.

REVIEW
Oxford Dictionary Definition

noun

formal assessment of something with the intention of instituting change if necessary:

Law a reconsideration of a judgement, sentence, etc. by a higher court or authority:

critical appraisal of a book, play, film, etc. published in a newspaper or magazine:

verb

[with object] assess (something) formally with the intention of instituting change if necessary:

What is a Review?

- A Review seeks to ensure that the Measures of the Security Plan, the Security Assessment, Operational Procedures and Practice are effective in meeting the Objectives of SOLAS XI-2, the Code and required legislation.
- IS IT FIT FOR PURPOSE ?????

Review versus Audit

- There are similarities between an Audit and a Review but they are NOT the same.
- The Review is focused on identifying the suitability of the system and its effective workings.

Administration Review

- Part A 9.2
  The Administration may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to recognised security organisations.
- 9.2.1
  In such cases the recognised security organisation, undertaking the review and approval of a ship security plan, or its amendments, for a specific ship shall not have been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review.

SSP A9.4

- The Plan shall address;-
  .11 procedures for the periodic review of the plan and for updating;

9.53 Audit and Review

- 9.53 The SSP should establish how the CSO and the SSO intend to audit the continued effectiveness of the SSP and the procedure to be followed to review, update or amend the SSP.

Non compliance

- 9.8.1 If the officers duly authorised by a Contracting Government have clear grounds to believe that the ship is not in compliance with the requirements of chapter XI-2 or part A of this Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the ship security plan, limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Contracting Government of, or the master of, the ship concerned. Nevertheless, the provisions in the plan relating to section 9.4 subsections .2, .4, .5, .7, .15, .17 and .18 of this part of the Code are considered as confidential information, and cannot be subject to inspection unless otherwise agreed by the Contracting Governments concerned.

Part A **10 RECORDS**

- 10.1 Records of the following activities addressed in the ship security plan shall be kept on board for at least the minimum period specified by the Administration, bearing in mind the provisions of regulation XI-2/9.2.3:.....

  .6 internal audits and reviews of security activities;
  .7 periodic review of the ship security assessment;
  .8 periodic review of the ship security plan;
  .9 implementation of any amendments to the plan; and

A 11.2 CSO Responsibilities

- 11.2 In addition to those specified elsewhere in this part of the Code, the duties and responsibilities of the company security officer shall include, but are not limited to:

  .5 arranging for internal audits and reviews of security activities;
  .6 arranging for the initial and subsequent verifications of the ship by the Administration or the recognised security organisation;
  .7 ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance a are promptly addressed and dealt with;

A12.2 SSO RESPONSIBILITIES

- 12.2 In addition to those specified elsewhere in this part of the Code, the duties and responsibilities of the ship security officer shall include, but are not limited to:

  .5 reporting to the Company Security Officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;

B. 8.13 SSA

- 8.13 If the SSA has not been carried out by the Company the report of the SSA should be reviewed and accepted by the CSO.

Part A 8.5

- The ship security assessment shall be documented, reviewed, accepted and retained by the Company.

REVIEW AND RSO's

- 9.4 All SSPs should be approved by, or on behalf of, the Administration. If an Administration uses a Recognised Security Organisation (RSO) to review or approve the SSP the RSO should not be associated with any other RSO that prepared, or assisted in the preparation of, the plan.

B4.26 **Alternative Security Agreements**

- Contracting Governments, in considering how to implement chapter XI-2 and part A of this Code, may conclude one or more agreements with one or more Contracting Governments. The scope of an agreement is limited to short international voyages on fixed routes between port facilities in the territory of the parties to the agreement. When concluding an agreement, and thereafter, the Contracting Governments
- The operation of each agreement must be continually monitored and amended when the need arises and in any event should be reviewed every 5 years.

When to Review

- ?

REVIEW OF THE SECURITY PLAN

- Meeting the Contracting Government obligations, a framework is required.
- Example.....
  - UK - TRANSEC require that a Security Plan review should be taken at least every 6 months and MUST be reviewed when;
    - The relevance of the Security Assessment has been affected by Operational Changes.

Questions?

Lecture TWELVE
"Security Equipment"
13.1.5 13.1.16 Part B

SECURITY EQUIPMENT

Examples of Security Equipment and Systems

- GMDSS
- AIS
- Locks
- Lighting
- Booms
- Turnstiles/Gates/Barriers
- Fencing and Gates
- Razor/Barbed Wire
- Slippery Foam
- Radar
- Security Glass Film
- Water and Foam monitors
- Biometric Systems
- Perimeter Intrusion Devices (PIDS)
- Alarms
- Communication systems (Radios)
- Closed circuit TV
- Baggage screening equipment
- Under vehicle video (VV)
- Metal detectors (AMD, HHMD)
- Baggage X-ray equipment
- Container X-ray devices
- Explosive trace detection equipment
- Vapour & narcotics detection equipment
- Radiation detection devices
- Tracking Systems

GMDSS-Global Maritime Distress and Safety System

- An international system that uses terrestrial and satellite technology and ship-board radio systems to ensure rapid, automated alerting of shore-based communication and rescue authorities, in addition to ships in the immediate area
- All cargo ships of 300 gross registered tonnes and upwards and all passenger ships engaged on international voyages must be equipped with GMDSS.

World divided into four main sectors, each area having a system to support the use of GMDSS
Area 1....VHF DSC
Area 2....MF DSC
Area 3....INMARSAT/HF
Area 4... HF DSC

AIS

Automatic identification systems (AIS) are designed to be capable of providing information about the ship to other ships and to coastal authorities automatically every 6 hours.

Initially a Safety Measure, but can be used for Maritime Security

BOOMS & NETTING

Seaward Protection

RUNNING GEAR ENTANGLEMENT

- Running Gear Entanglement (RGE)
  - Provides the ability to stop surface craft
  - Deployed by 'line thrower' (non pyro)

Netting

- Dropped by Helicopter in front of suspect vessel

PERIMETER FENCING ?

BS1722 Part 10

CLIMBING FRAMES

FENCING WEAKNESSES

ELECTRIC FENCING




- Differing varieties.
- Commercial
- Discrete systems for Yachts

RAZOR WIRE/BARBED WIRE


- **Barbed Tape** or R**azor Wire** is a mesh of metal strips with sharp edges.
- Barbed Wire mesh of metal strips with sharp barbs protruding along the wire.
- Commonly used to re-enforce normal fencing whose purpose is to prevent passage by humans.
- However where Health and Safety Acts exist they must be considered before use and consent granted if required.

ACCESS CONTROL
GATE FEATURES 1

BARRIERS – WHAT BARRIERS ?


ACCESS CONTROL
GATE FEATURES 2

Infra Red Alarm Beams...


...Linked to CCTV.

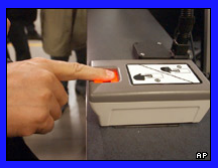
ACCESS CONTROL
GATE FEATURES 3

SIGNS

- Can give a strong signal about security awareness in a Port and on a Ship
- Can be a form of deterrent against unauthorised access
- Must be used to denote Restricted Areas
- At 50m intervals and on all access points
- Specific wording to comply with EC requirements (See notes)
- Must be used to advise where CCTV is used

KEY PAD ACCESS

BIOMETRIC IDENTITY VERIFICATION SYSTEMS



- Modern Technology
- Unique Identification
- Reliable
- Being introduced more frequently
- Recent U.S. Entry requirement

QUALITY LOCKS

BS 3621-1980.

- Locks are only any use if used correctly
- Should not be over relied upon

CYBER LOCKS

- Electronic versions of standard mechanical locks
- Cyber locks have no keyway and cannot be picked
- Not possible to duplicate cyber keys
- Keys can be programmed for the locks they can open, even to times and dates

DOOR SECURITY

DEADLOCK Electronic Door Controls

Panic Hardware

A range of heavy-duty panic hardware is available, designed with quality, reliability and elegance to suit virtually all egress control requirements.

Manufacturers ranges include Panic Bolts / Latches and Touch bars,

SHIPS ENVIRONMENT & SAFE EGRESS

DOOR SEALS 1

- It has a high tensile strength and any attempt at removal will result in the seal breaking

- Door seals for Container, ship, or buildings.

SECURITY GLASS FILM

Security films are applied to prevent glass from shattering.

Typically applied to commercial glass, these films are made of heavy-gauge plastic and are intended to maintain the integrity of glass when subject to heavy impact.

The most robust security films are capable of preventing fragmentation and the production of hazardous glass shards from forces such as bomb blasts. Some companies have even experimented with bullet ballistics of multiple layers of security film

WATER AND FOAM MONITORS

- MOST SHIPS HAVE THE CAPABILITY TO EFFECTIVELY REPEL UNLAWFUL BOARDERS THROUGH THE USE OF WATER HOSES.
- WATER AND FOAM MONITORS ALTHOUGH LESS FLEXIBLE COULD ALSO BE USED.

SLIPPERY FOAM

- The Mobility Denial System is an oil-slick-in-a-can, a combination of "Drilling Mud Additive, Flocculent and water" that renders surfaces as slippery as wet ice.
- This was trialed in the US for the Military, however on further investigation it was ascertained that it required to much water to make effective, and was not pursued.

- To date although viable as a security measure, Slippery Foam has not yet been massed produced or used in public.

RADAR

- Short Range – Close Monitoring

PORT LIGHTING

- Quality Security lighting has several Benefits;
  - Acts as a deterrent to unauthorised intruders.
  - Assists in visual observation of strategic areas and perimeters
  - Supports other detection methods (CCTV)
  - Reliable / low cost
  - Consider
    - The minimum lighting level (LUX)
    - Potential hazards caused by poor sighting of light units. (ship night vision, local environment etc)
    - Lighting stanchions being used as climbing aids.

SHIPBOARD LIGHTING

- ADEQUATE LIGHTING LEVELS
- OVER SIDE LIGHTING
- PARTICULARLY IMPORTANT IN AREAS OF CCTV COVERAGE
- SAFETY OF NAVIGATION TO BE CONSIDERED

LOW LIGHT DETECTION

- A good watch in high threat areas
  - Equipped with high powered binoculars
  - Night Vision Aids
    - Majority of attacks take place at night or early morning

ALARM SYSTEMS

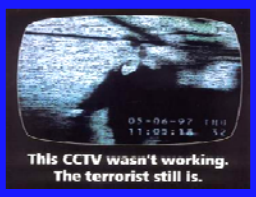
- Control Panel: Keypad: Siren:
- Inside Motion Detector:
  - Passive infrared, microwave, or photoelectric detectors sense changes in a room caused by human presence..
- Door and Window Contacts: Magnetic contacts
- Central Monitoring Station (Company):.
- Smoke Detectors
- Glass Break Detectors
- Panic Buttons silent alarm or sound the alarms within the area.
- Pressure Mats.
- Linked with Closed circuit TV
- Alarm Screens
  - special wire woven in the mesh that will activate an alarm when cut or removed.

PERIMETER INTRUSION DETECTION SYSTEM

CCTV TYPES

- Standard CCTV Surveillance Cameras
- Dome CCTV Cameras
- Covert & Concealed Surveillance Cameras
- PTZ flexibility

CCTV



System Operational?
Adequate lighting?
Planned Maintenance Schedule?
Regular Tape Changes/ Digital Archiving?
Lenses clean?

CC – TV Operator

MONITORING VULNERABLE AREAS
CCTV

SCREENING EQUIPMENT

- Come in many different guises
- Metal Detectors
- Vapour Detectors
- X-Ray Systems

- These systems must be augmented by a physical search of a set proportion of those being screened.
- B 9.38/B16.45
  - Double screening not envisaged. If Port equipped then responsibility to screen lies with the Port.

METAL DETECTORS

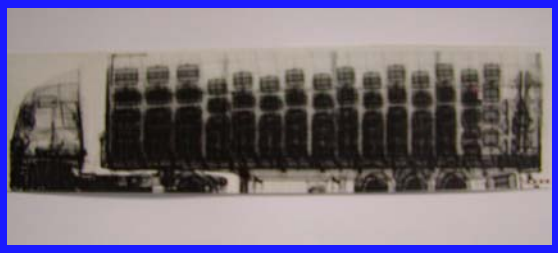
AMD – HHMD
Environment &
Calibration
Limitations

X-RAY SCANNERS

X-RAY INTERPRETATION

CONTAINER SCANNING

X-RAY SYSTEMS (Truck)



TOP AND BACK VERTICAL LAYER ORDINARY T.V.'S BOTTOM LAYERS FILLED WITH DRUGS

EXPLOSIVE DETECTION

BOMB SUPRESSION

- BOMB BLANKETS
- BLAST SUPRESSION BINS

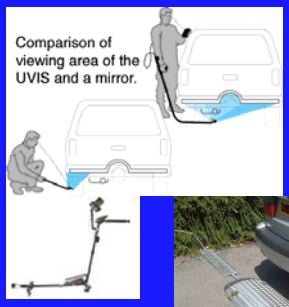
1 kg TNT Uninhibited & Inhibited

VAPOUR AND NARCOTICS DETECTION

RADIOACTIVE DETECTION

- Covert and Overt Systems
- New devices being developed in the maritime and aviation sectors
- Soon to be deployed in Major UK ports for freight

UNDER VEHICLE VIDEO (UVV)



TRACKING SYSTEMS

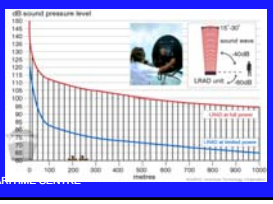
- Logistics
- Vehicles
- People
- Localised and Global systems
- Container Tracking
- Electronic tagging

COMMUNICATION SYSTEMS

- Robust
- Secure
- Privacy
- Backed Up
- Quality communication is essential for Security Staff within the facility and between the Ship and Port Facility
- Staff in control of CCTV should be able to communicate to Security Staff at all times, therefore in both cases hand held radios should strongly be considered, were possible with dedicated and encrypted channels.

Long Range Acoustic Device LRAD

- On full power, the device can emit a concentrated, 150 decibel [dB] high energy acoustic wave, which retains a level of 100dB over distances of 500 metres. Supersonic airliner Concorde emitted about 110dB, most household smoke detectors about 85dB
- The wave is focused within a 15-30 degree 'beam', allowing the LRAD to be aimed at a specific target
- Persons standing next to the wave will experience 40dB less noise than those directly in its path. Those behind the LRAD unit are shielded by a 60dB reduction in output



MAGNETIC AUDIO DEVICES

- Acoustic Devices
  - Magnetic Audio Devices (MAD)
  - Provide distant (700mtrs – 12kms) hailing and warning
  - Small and compact
  - Not classed as a lethal weapon

TESTING, CALIBRATION & MAINTENANCE OF SYSTEMS

Part B 13.3.9 & 18.2.8

Consideration should be given to;

- Procedures to ensure Operational readiness
- Routine tests undertaken
- Appropriate training of skilled Operators
- Drills in use of equipment
- Planned Maintenance procedures to ensure continuing accuracy
- Back-up provisions
- Maintenance and inspection records
- For ships; security equipment should be maintained in line with the provisions of Section 10 of the ISM Code

OPERATIONAL LIMITATIONS OF SECURITY EQUIPMENT & SYSTEMS

Functional and operating constraints may include:-

- Effective Ranges
- Environmental sensitivities
- Lighting, Power supplies
- Operating human errors (Training)

TECHNIQUES USED TO CIRCUMVENT SECURITY MEASURES

No security equipment is infallible and techniques can be employed to evade security systems such as:

- Disabling alarm systems
- Isolating electrical supply
- Physical Removal
- Coercion
- Poor Security Management (Documentation)

Anti Piracy
Use of Armed Guards

Newly adopted guidance at MSC 90 (25 May 2012) - MSC.1/Circ.1443 Interim guidance to private maritime security companies providing privately contracted armed security personnel on board ships in the High Risk Area

Newly adopted guidance at MSC 90 (25 May 2012) - MSC.1/Circ.1405/Rev.2 Revised Interim guidance to shipowners, ship operators and shipmaster on the use of privately contracted armed security personnel on board ships in the High Risk Area (revokes MSC. 1/Circ.1405/Rev.1)

Questions?

Summary & Review Day 3