

## Day 4 Questions related to DAY THREE



© LAIRDSIDE MARITIME CENTRE

## Web Sites as promised

- <http://www.dft.gov.uk/publications/ship-security-plan-template>
- [http://www.dft.gov.uk/mca/mcga07-home/shipsandcargoes/mcga-shipsregsandguidance/mcga\\_dops\\_maritimesecurity\\_mainpage/dops\\_ms-guidance/mcga\\_dops\\_msb\\_ssp/dops\\_msb\\_model\\_ship\\_security\\_plan.htm](http://www.dft.gov.uk/mca/mcga07-home/shipsandcargoes/mcga-shipsregsandguidance/mcga_dops_maritimesecurity_mainpage/dops_ms-guidance/mcga_dops_msb_ssp/dops_msb_model_ship_security_plan.htm)

© LAIRDSIDE MARITIME CENTRE



## Lecture THIRTEEN "Security Actions"

© LAIRDSIDE MARITIME CENTRE

## IMO Guidance

- MSC/Circ.1111
- 7 June 2004
- GUIDANCE RELATING TO THE IMPLEMENTATION OF SOLAS CHAPTER XI-2 AND THE ISPS CODE

© LAIRDSIDE MARITIME CENTRE

## MSC 1111:2004

When visiting a ship for the purpose of regulation XI-2/9 consider:-

- When approaching, boarding and moving around the ship note the Security measures in regard to
  - Access Control
  - Searching
  - Segregation of Embarking/disembarking Passengers
  - Security of unattended spaces
  - RA's marked
  - Bridge/E.R/RA's capable of being locked
  - Deck Watches in place
  - Monitor landward/Seaward approaches
  - Checking of Stores & Securely stored
  - Checks and scanning of Cargo
  - Cargo Checked against Documentation
  - Seals and anti-tampering methods checked
  - .....etc

© LAIRDSIDE MARITIME CENTRE

## Ship – Port Facility Interface

- As we have seen, the Code applies at the Ship-Port facility interface
- Therefore ships measures should be considered in respect of the environment in which the ship operates i.e.
  - does it always interface in a Port Restricted Area?
  - What reciprocal agreements are in place between ship and port facility?
  - Are there any specific measures addressed by a DOS?
  - Are the Level Measures compatible?
  - Is there good communication and co-operation between ship and port facility?

© LAIRDSIDE MARITIME CENTRE

## Verification of the Ship Security Measures

- ❑ *Clear grounds* that the ship is not in compliance means evidence or reliable information that the security system and any associated security equipment of the ship does not correspond with the requirements of SOLAS chapter XI-2 or part A of the ISPS Code, taking into account the guidance given in part B of the ISPS Code.
- ❑ Such evidence or reliable information may arise from the duly authorized officer's professional judgment or observations gained while verifying the ship's International Ship Security Certificate or Interim International Ship Security Certificate issued in accordance with part A of the ISPS Code or from other sources.
- ❑ Even if a valid certificate is on board the ship, the duly authorized officers may still have clear grounds for believing that the ship is not in compliance based on their professional judgment (ISPS Code paragraph B/4.32).

© LAIRDSIDE MARITIME CENTRE

## SECURITY LEVELS

RECALL.....

The ISPS Code defines THREE SECURITY LEVELS.....

### ❑ SECURITY LEVEL 1

*LEVEL AT WHICH THE SHIP / PORT NORMALLY OPERATES.*

### ❑ SECURITY LEVEL 2

*HEIGHTENED LEVEL OF SECURITY DUE TO INCREASED RISK OF SECURITY INCIDENT.*

### ❑ SECURITY LEVEL 3

*IMMEDIATE OR IMMINENT THREAT.*

CONTRACTING GOVERNMENTS WILL OFFICIALLY SET SECURITY LEVELS

© LAIRDSIDE MARITIME CENTRE

Identify threats... establish proportionate security measures



© LAIRDSIDE MARITIME CENTRE

## THE THREAT

*Part B. 8.9 / 15.11*

- ❑ Damage/destruction of the Ship or Port facility
- ❑ Hijacking of the ship
- ❑ Tampering with cargo/stores etc on board or in the facility
- ❑ Unauthorised access/ stowaways etc
- ❑ Smuggling weapons etc, including WMD
- ❑ Use of ship to carry those intending to carry out a security incident or their equipment
- ❑ Use of the ship as a weapon
- ❑ Attacks from seaward while at berth/anchor
- ❑ Attacks at sea
- ❑ &c &c.

© LAIRDSIDE MARITIME CENTRE

## SECURITY LEVEL CHANGES

- ❑ HOW IS THIS IMPLEMENTED?
- ❑ UK Methodology
  - TRANSEC will advise the CSO and Port Facilities of changes to security levels by Fax.
  - CSO's and Ports must have a Fax machine capable of receiving faxes on a 24 hours basis.
  - The machine should be maintained and regularly checked for incoming faxes

© LAIRDSIDE MARITIME CENTRE

## PRIOR NOTIFICATION PROCEDURES

- ❑ Mandated by EU Regulation 725:2004 Art 6 Annex 1 (Ch XI-2 Reg 9.2 SOLAS)
- ❑ 4 Staged process – principally PFSO led
  1. PFSO Data Collection
    - Consideration of responses – Government to give Guidance
    - Ship - ISPS Compliant / ISSC issued and is it current?
  2. Application of Government control measures as required
  3. Port Pre Arrival Information obtained
  4. Apply PFSO Procedures as per PFSP

© LAIRDSIDE MARITIME CENTRE

## Reporting Form

- ❑ See Page 39-40 of Notes.
- ❑ SHIP PRE-ARRIVAL SECURITY INFORMATION FORM

© LAIRDSIDE MARITIME CENTRE

## ENTERING A FOREIGN PORT

- ❑ Ships intending to enter a foreign port may be required to provide information to the port state, including:
  - confirmation that the ship possesses a valid ISSC;
  - the Security Level at which the ship is operating;
  - the Security Level at which the ship operated in at the last ten ports of call;
  - any special or additional security measures undertaken at the last ten ports of call;
  - confirmation that appropriate procedures were maintained during any ship-to-ship activity between the last ten ports of call;
  - other practical security related information.

© LAIRDSIDE MARITIME CENTRE

## MAINTAINING SECURITY OF SHIP AND PORT INTERFACE

The Ship Security Plan must be able to interface with the Port Facility Security Plan:

- ❑ The setting of security requirements between the ship and the port must be in liaison between the CSO, PFSO and SSO to understand their duties and constraints.
- ❑ If the port is at a higher level of security than the ship, then the ship will have to increase its security level in line with the port.

© LAIRDSIDE MARITIME CENTRE

## IMPLEMENTATION OF SECURITY PROCEDURES

- ❑ THE ISPS CODE "PART B"

SECTIONS 9.9 TO 9.49 COVERS THE SHIP IMPLEMENTATION IN PRACTICE

SECTIONS 16.17 TO 16.63 COVERS THE PORT FACILITY IMPLEMENTATION IN PRACTICE

© LAIRDSIDE MARITIME CENTRE

## COMMUNICATIONS

- ❑ Effective communication Channels between Port facility and Ship are essential
- ❑ Port facilities must be aware of the Security level on any ship intending to enter the Port facility.
- ❑ Details should be exchanged at the earliest opportunity.
  - Port entry reporting?
  - Verification?
- ❑ Effective communications between Security Personnel in the facility are also essential.
- ❑ Appropriate and effective communication methods are particularly important at Security Level 2.
- ❑ Back-up systems should be available.

© LAIRDSIDE MARITIME CENTRE

## THE DECLARATION OF SECURITY 1

- ❑ THE MAIN PURPOSE IS TO:
  - Ensure agreement is reached between the port facility and the ship. Respective security will be undertaken in accordance with the respective security plans.
  - Contracting government for the port may request a DOS is completed when deemed necessary.

© LAIRDSIDE MARITIME CENTRE

## THE DECLARATION OF SECURITY 2

- ❑ May be requested when:
  - A non SOLAS Ship requires entry to the Port
  - In ALL cases when the Port Facility or Ship are operating at level 3
  - When the ship is at a higher level than the port or another ship alongside
  - Following a Security Incident or security threat
  - When a Contracting Government deems it to be necessary
  - As required under the SSP/ PFSP
  - Combination of the above factors

© LAIRDSE MARITIME CENTRE

## DOS

### Procedures for Port Facilities

- ❑ When the Port Facility requires a DoS, the PFSO should;
  - Contact the Ship's SSO/Master Prior to Port entry
  - Establish the Security Level of the Ship and Port
  - Obtain details of Security Measures the ships intends to carry out
  - Draw up details of security measures the Port will put in place
  - Agree measures with the SSO to ensure the highest security level is met.

© LAIRDSE MARITIME CENTRE

## SHIP REQUEST FOR A DoS

As per requirement of Part A - Paragraph 5.2 of the Code.

- ❑ the ship is operating at a higher security level than the port facility or another ship it is interfacing with;
- ❑ there is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;
- ❑ there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;
- ❑ the ship is at a port which is not required to have and implement an approved port facility security plan; or
- ❑ the ship is conducting ship to ship activities with another ship not required to have and implement an approved ship security plan.

© LAIRDSE MARITIME CENTRE

## MSC/Circ.1132 14 December 2004

### Para 12

Though a ship has to comply with a request from a port facility to complete a DoS, a port facility does not have to comply with a request for the completion of a DoS from a ship, though a request from a ship to complete a DoS has to be acknowledged by the port facility (section A/5.3 of the ISPS Code).

In the same way another ship does not have to comply with the request for a DoS though it should acknowledge receipt of the request (section A/5.3 of the ISPS Code).

© LAIRDSE MARITIME CENTRE

## MSC/Circ.1132 14 December 2004

### Para 13

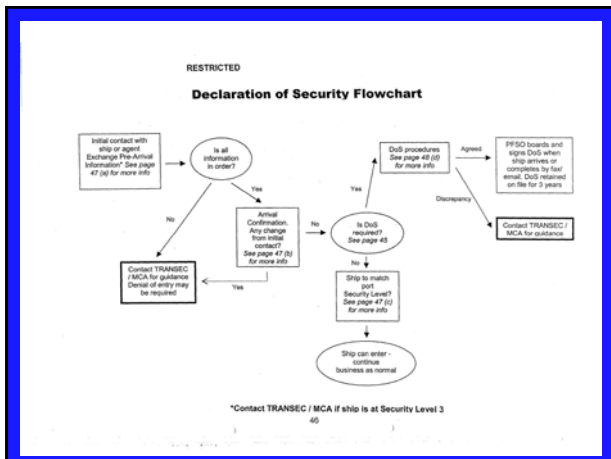
The DoS is intended to be used in exceptional cases usually related to higher risk, when there is a need to reach an agreement between the port facility and the ship as to the security measures to be applied during the ship/port interface because, either the provisions of the PFSP and of the SSP did not envisage the situation or SOLAS chapter XI-2 and part A of the ISPS Code have not anticipated the specific circumstances as listed in section A/5.2 of the ISPS Code. There should be a security-related reason relating to the specific ship/port interface or ship-to-ship activity for requiring or requesting completion of a DoS.

© LAIRDSE MARITIME CENTRE

## DoS ADMINISTRATION

- ❑ Ensure that the form of DoS accords with the Model in annex D of the ISPS Code
- ❑ Complete the DoS for signature by all Parties: SSO, Master, PFSO. Officers of Contracting Govt's as required. The DOS is required to be retained for inspection
- ❑ DoS records should be retained by both PFSO and SSO for a period specified by their contracting government.(UK Minimum of **3 years** for both ports and ships.
- ❑ Different requirements elsewhere e.g. Croatia 6 months or 10 port calls.
- ❑ In the case of Ships any DoS relating to one of last ten ports of call shall be retained as long as it relates to any of those last 10 ports of call even if the period over which those calls extend exceeds the minimum period.

© LAIRDSE MARITIME CENTRE



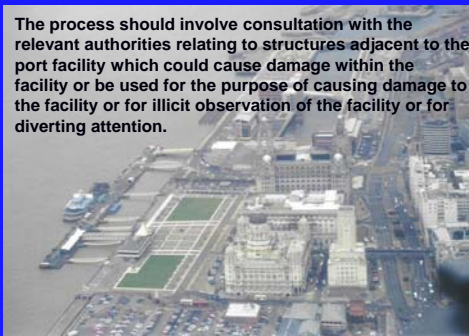
## Ship & Port Environment

- How should the ship manage its Security in respect of the Port Environment?
- ISSUES FOR SHIPS WHEN INTERFACING WITH A PORT FACILITY

© LAIRDSE MARITIME CENTRE

## PORT FACILITY ENVIRONMENT Sect 15.12 Part B

The process should involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.



© LAIRDSE MARITIME CENTRE

## ACCESS Discussion ?

- HOW DO GENERAL PORT ACTIVITIES AFFECT THE SHIP SECURITY?

- Anglers (Fishermen)
- Photographers
- Boat Spotters
- Rights of Way
- Dwellings and Businesses

HOW SHOULD/CAN THESE ISSUES BE MANAGED ?

When should these issues be considered.

© LAIRDSE MARITIME CENTRE

## PUBLIC RIGHTS OF WAY Before ISPS



© LAIRDSE MARITIME CENTRE

## PUBLIC RIGHTS OF WAY After

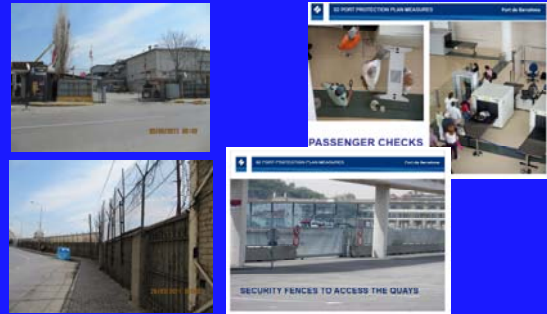


## Fences & Signs



© LAIRDSIDE MARITIME CENTRE

## How do other member states control Access?



© LAIRDSIDE MARITIME CENTRE

## PUBLIC RIGHTS OF WAY

### UK Position

- ❑ May be suspended following a direction under EU725:2004 where such a Right of way represents a palpable security risk to the Port facility by increasing its vulnerability.

© LAIRDSIDE MARITIME CENTRE

## SHIPS CREW Shore Leave

IMO Amendments to SOLAS 1974. Conference 12 Dec 2002. Resolution 11.

Additional Guidance in IMO MCS1342 May 2010

- ❑ The rights and needs of Seafarers need to be considered throughout
- ❑ Measures should not unduly inhibit access to shore facilities, shore leave and the reception of visitors.
- ❑ Consideration should be given to pass systems and searches
- ❑ Not to be subjected to more frequent or intrusive checks than others having access to the Port facility.

© LAIRDSIDE MARITIME CENTRE

## SHIPS CREW ID

- ❑ In identifying Ships Crew and number of methods may be considered:-
  - MASTER/AGENT provide a Crew List prior to arrival
  - Individuals identification by
    - Passport
    - Ships Crew Company pass
    - Proof that the Master has granted Shore Leave

The ILO International Seafarers ID may overcome these difficulties.

© LAIRDSIDE MARITIME CENTRE

## AUTHORISED OFFICIALS ID

- ❑ Official ID Definition
 

Documentation that officially identifies the Holder as a person who has legitimate right of access into an R.A, such as Police Warrant Cards, Government Security Inspectors Passes.
- ❑ Details of Official ID Documents would normally be used during Training Courses to Port Facility Staff are familiar with Pass types.
- ❑ Exceptions may be agreed locally and must be included in the PFSP.

© LAIRDSIDE MARITIME CENTRE



## ACCESS CONTROL PASS SYSTEMS



## ACCEPTED PASSES

- ❑ Consideration should be given to Pass systems and who have requirements for access to R.A's e.g Ships Pilots
- ❑ If the PFSO agrees to accept other passes, this must be recorded in the PFSP

© LAIRDSIDE MARITIME CENTRE

## PILOT IDENTIFICATION

- ❑ 17.2.13 Part A, requires PFSO's assist SSO's in confirming the ID of those seeking to board the ship and 9.14 Part B requires the SSP has measures to check the identity of all persons seeking to board the ship.
- ❑ Delays can result in boarding a Pilot
- ❑ Name of a Pilot should be communicated to the ship by secure method from the Port Authority
- ❑ Pilot should confirm Identity against that communicated with Photographic Pass

© LAIRDSIDE MARITIME CENTRE

## SEARCHING

- ❑ Requirements will differ on Ship or Port Classification
- ❑ Are staff with full RA Access generally required to be subject to physical search?
- ❑ At times when Security measures may need to be enhanced does the Contracting Government apply additional measures without moving to a higher level. *(Example TRANSEC may require set a search throughput regime)*
- ❑ Measures must be proportionate and responsive

© LAIRDSIDE MARITIME CENTRE

## VEHICLE PARKING

- ❑ All Vehicle Parking within the Ship/Port interface area should be controlled and restricted. Ships crew should be aware of the environment in which they operate
- ❑ Example
  - Differing requirements for each Port Classification in terms of Vehicle passes but.
  - At LEVEL 2 vehicle access should be restricted and limited to those with valid Vehicle passes
  - Passes should be clearly displayed and be regularly checked by Security Patrols
  - At LEVEL 3 non-essential Vehicle Parking should be prohibited and limited to Key Staff.

© LAIRDSIDE MARITIME CENTRE

## HANDLING OF THE NEWS MEDIA

- ❑ It is of paramount importance that all security related enquiries by the media are controlled.
- ❑ Enquiries can be directed either to one person appointed as a spokesperson or to a department.
- ❑ All other persons should be instructed not to discuss any situation with outsiders, especially the news media.
- ❑ Ensure that the news media be furnished with accurate information and that additional security threats are not precipitated by irresponsible statements from uninformed sources.

© LAIRDSIDE MARITIME CENTRE

## SECURITY MEASURES

- ❑ Protection of Assets
  - Identify the Threat
  - Prevention first defence
    - Detect and Deter
  - Information – current trends, Security Intelligence availability
  - Ensuring Security Shipboard personnel adequately briefed
  - Use of Profiling ????
  - and...
  - The ongoing provision of shipboard security

© LAIRDSIDE MARITIME CENTRE

## PROTECTION & PREVENTION

- ❑ Illuminations
- ❑ Barbed Wire
- ❑ Fencing
- ❑ Securing all access points
- ❑ Repelling boarder techniques
- ❑ Maintaining all security equipment
- ❑ Good liaison with Port Facilities
- ❑ Patrolling
- ❑ Securing unused spaces
- ❑ Visitor control
- ❑ Restricted area management; cargo, potable water,
- ❑ Stores, bridge, accommodation etc

© LAIRDSIDE MARITIME CENTRE

## AWARENESS PROTOCOL

- ❑ IS IT.....
- ❑ HIDDEN
- ❑ OBVIOUSLY SUSPICIOUS
- ❑ TYPICAL IN ITS LOCATION

HOT

© LAIRDSIDE MARITIME CENTRE

## SEARCH METHODOLOGY

- ❑ Ships should have a reference – (Port plans, drawings, photos etc).
- ❑ Prioritise:
- ❑ Required with regard to
  - PEOPLE (9.14) (16.14)
  - PERSONAL EFFECTS (9.14.2) (16.14)
  - BAGGAGE (9.14.2 & 9.38) (16.46)
  - VEHICLES (9.14.3) (16.14)
  - SHIPS STORES (9.33) (16.40)
  - CARGO (9.25) (16.32)
- ❑ At ALL SECURITY LEVELS
- ❑ Regular Patrols in Place

- *That should not be there*
- *That can not be accounted for*
- *That is out of place*

© LAIRDSIDE MARITIME CENTRE

## PROTECTION & PREVENTION Basic

*Deter – detect – react!*

- |   |  |
|---|--|
| • Vigilance   | • Gangway Access manned/monitored  |
| • Professional Patrols  |  |
| • Close range radar monitoring. AIS                                 | • Raise pilot ladders, gangways, etc   |
| • Good Quayside lighting. Searchlights and ship over-side lighting. | • CCTV Observation   |
|   | • Observing cables and mooring lines. Defence mechanisms deployed (rat guards) |

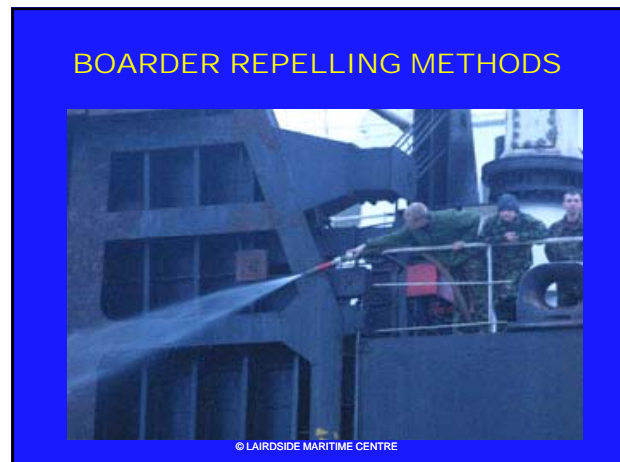
© LAIRDSIDE MARITIME CENTRE

## AREAS FOR CONCEALMENT

- |  |   |
|--|---|
| ❑ Behind Cabinets                                | ❑ Inside Coat hangers                     |
| ❑ Inside Radios and Recorders                    | ❑ Inside rolled socks                     |
| ❑ Cargo Containers                               | ❑ Hollowed out moulding                   |
| ❑ Ventilator ducts                               | ❑ Wire Harness                            |
| ❑ Storage Tanks                                  | ❑ Railings                                |
| ❑ Heater Units                                   | ❑ Fire Extinguishers, Hoses, compartments |
| ❑ Above/behind light fittings                    | ❑ Access Panels                           |
| ❑ Above and behind wall panels                   | ❑ Behind/inside water coolers             |
| ❑ False bottom clothes, suitcases, hanging units | ❑ Behind wash basins and toilets,         |
|  | ❑ Towel dispensers                        |
|  | ❑ Taped to shower units and pipes         |

© LAIRDSIDE MARITIME CENTRE



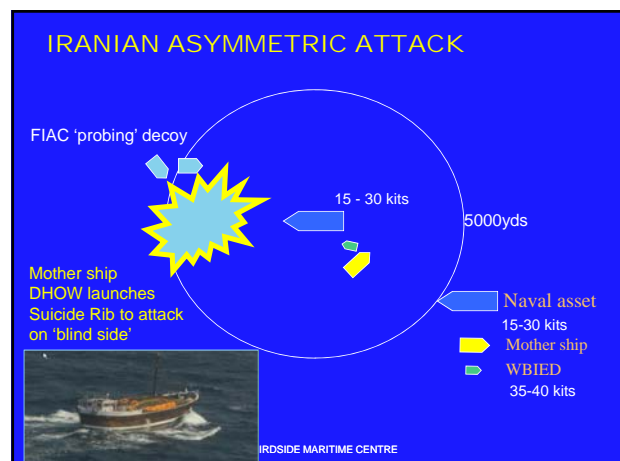


### ATTACK BY TROJAN HORSE

- "Any vehicle likely to go unnoticed in a particular environment designed to be used to mount a Terrorist attack from within."
- E.g. POLICE VEHICLE, FIRE, AMBULANCE, UTILITY VEHICLES, TAXI'S, REGULAR FACILITY TRADERS.

Source SO13 Met Police.

© LAIRDSIDE MARITIME CENTRE



## MINING THREAT TO SHIPS & PORTS



## ANCHORAGES & LAY-BY BERTHS

- ❑ From the Definition of a Port Facility Anchorages can be designated as Port Facilities
  - UK not presently applying security measures – under review.
  - Other states????
- ❑ Ships are responsible for their own Security and may record anchorage time as one of their 10 Port calls
- ❑ At Lay-by berths Ships are responsible for their own Security at Level 1 but at Levels 2 and 3 Access must be controlled by the Port Facility

© LAIRDSE MARITIME CENTRE

## TRANSITING COASTAL AREAS UK Vessels example

- ❑ Heightened levels of Security may be needed when Transiting Coastal areas (m.v Limburg)
- ❑ Within 24nm of the Coast UK Ships should adopt the Security level in force for the geographical area or for the Country's level if higher
- ❑ Within 24nm Coastal States may expect ships to recognise their jurisdiction
- ❑ Further from shore the risk is considered to diminish

© LAIRDSE MARITIME CENTRE

## OPEN OCEAN

- ❑ Threat level in Open waters considered low. UK Ships unless advised otherwise adopt Security Level 1 measures
- ❑ Ships should comply with the Security Levels set by other Administrations whilst operating within these Sea areas where the level is Higher.

© LAIRDSE MARITIME CENTRE

## ISSC

- ❑ Issued by the Administration
- ❑ Valid for up to FIVE Years
- ❑ CERTIFIES:-
  - ❑ that the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of part A of the ISPS Code;
  - ❑ that the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A of the ISPS Code;
  - ❑ that the ship is provided with an approved Ship Security Plan.

© LAIRDSE MARITIME CENTRE

## SOLAS AMENDMENTS

### SOLAS V

- ❑ **AUTOMATIC IDENTIFICATION SYSTEM, (AIS)**  
AIS TO BE FITTED TO ALL SHIPS >300GT NOT LATER THAN 1<sup>ST</sup> S.E.C AFTER 1<sup>ST</sup> JULY 2004 OR 31 DECEMBER 2004 WHICHEVER OCCURS FIRST

### SOLAS XI

- ❑ **SHIP SECURITY ALERT SYSTEM**  
(PASSENGER SHIPS, TANKERS, BULK CARRIERS AND H.S. CARGO SHIPS NOT LATER THAN 1<sup>ST</sup> RADIO SURVEY AFTER 1<sup>ST</sup> JULY 2004. CARGO SHIPS > 500GT & MODUS NOT LATER THAN 1<sup>ST</sup> JULY 2006).
- ❑ **CONTINUOUS SYNOPSIS REPORT (CSR)**
- ❑ **SHIP IDENTIFICATION NUMBER**  
(SEVEN DIGIT NUMBER TO BE MARKED ON HULL EXTERNALLY AND INTERNALLY BY 1<sup>ST</sup> DID AFTER 1<sup>ST</sup> JULY 2004. PASSENGER SHIP > 100GT OTHER SHIPS > 300GT)

© LAIRDSE MARITIME CENTRE

## MSC/Circ.1072 26 June 2003

### GUIDANCE ON PROVISION OF SHIP SECURITY ALERT SYSTEMS

Possible methods of achieving the alert are as follows:

1. a system may employ proprietary tracking equipment.....
2. a system may utilise modifications of GMDSS equipment.\* .....not possible to confuse it with a GMDSS distress, urgency or safety alert; and
3. a system may utilise the exchange of messages containing key words between a ship and, typically, the Company.

This list is not intended as exhaustive and is not intended to inhibit future developments.

© LAIRDSIDE MARITIME CENTRE

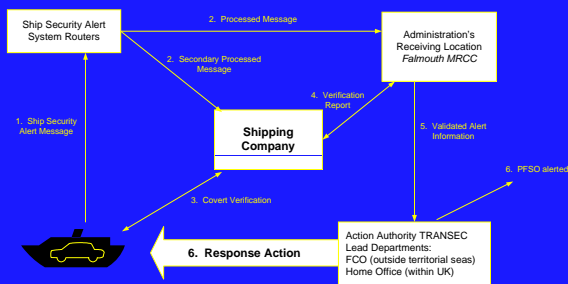
## SHIP SECURITY ALERT IN PORT

- Ships are required to fit a Ship Alert System not later than 1<sup>st</sup> July 2006.
- Systems will alert the a competent authority rather than the Port
- If a Ship Alert is initiated and verified, a Port will notified immediately



© LAIRDSIDE MARITIME CENTRE

### SHIP SECURITY ALERT SYSTEM



Source:

© LAIRDSIDE MARITIME CENTRE

## MSC/Circ.1073 10 June 2003 T2-NAVSEC/11

### MEASURES TO ENHANCE MARITIME SECURITY

- DIRECTIVES FOR MARITIME RESCUE CO-ORDINATION CENTRES (MRCCS) ON ACTS OF VIOLENCE AGAINST SHIPS

© LAIRDSIDE MARITIME CENTRE

## RESPONSE AGENCIES & CONTROL AUTHORITIES

□ ???

□ In the UK:

- TRANSEC
- MCA
- Local Police/SB
- HM Customs and Excise
- Immigration Service
- MoD

Ship and Port Facilities must keep up to date contact details for all the relevant response agencies to ensure rapid communication

© LAIRDSIDE MARITIME CENTRE

## The Response?



© LAIRDSIDE MARITIME CENTRE

## MSC Circ 1192/2006

- ❑ **THIS CIRCULAR PROVIDES GUIDANCE ON THE PROVISION OF INFORMATION FOR IDENTIFYING SHIPS WHEN TRANSMITTING SHIP SECURITY ALERTS**
- ❑ A ship security alert systems must function in an effective and efficient manner so as to provide the security-related benefits for which they were envisioned,

© LAIRDSIDE MARITIME CENTRE

## LRIT

- ❑ A number of MSC Circulars, MSC 1294 to 1298 and also MSC 1307 provide various guidelines on the provision of LRIT.
- ❑ Of particular note are MSC 1296 and MSC 1307 provide Guidance on **"THE SURVEY AND CERTIFICATION OF COMPLIANCE OF SHIPS WITH THE REQUIREMENT TO TRANSMIT LRIT INFORMATION"**

© LAIRDSIDE MARITIME CENTRE

Questions?

© LAIRDSIDE MARITIME CENTRE

COFFEE

© LAIRDSIDE MARITIME CENTRE

## EXERCISE 4 OPERATION 'DIGITAL'

© LAIRDSIDE MARITIME CENTRE

Questions?

© LAIRDSIDE MARITIME CENTRE

## SUPPLY CHAIN SECURITY



## SUPPLY CHAIN SECURITY

USA – Main drivers behind Supply Chain Security, through the following initiatives:

- 24 Hour Advance Vessel Manifest Rule
- Container Security Initiative
- Customs – Trade Partnership Against Terrorism (C-TPAT)
- Secure Freight Initiative

## 24 Hour rule

**Aim:** From February 2003 -Risk analysis – stopping high risk cargo entering US

- ❑ Obligations on all carriers loading cargo destined for US (C-TPAT carriers not exempt)
- ❑ Submit cargo manifest date 24 hours prior to loading (long and short haul)
- ❑ 14 data elements transmitted to National Targeting Center in US
- ❑ Applies to containerised cargo, and break bulk
- ❑ Empty containers only container numbers to be filed before arrival
- ❑ Bulk cargo exempt.

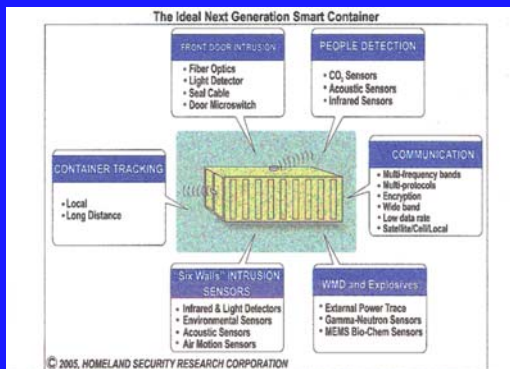
## CONTAINER SECURITY INITIATIVE

- Launched 2002 – incorporated in Safe Port Act 2006
- Aim pre screen cargo abroad – avoid loading of risk cargo without further examination
- US personnel posted at foreign ports assess risk using:
  - Filings under 24 hour Rule (Automated Targeting System)
  - Non-Intrusive Inspection
- Protocols agreed with host country to handle high risk containers

## CONTAINER SECURITY INITIATIVE

- Why become a CSI port?
  - First Ports to resume trade with US after terrorist incident
  - Use down time at port of loading and save time upon arrival in US (in theory)
  - Possible reciprocity for US outbound containers (Japan, Canada)
- 52 Ports end of August 2007 – 58 planned for end of 2007 (23 of these in EU)

## SMART CONTAINER OF THE FUTURE



## CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

- Introduced 2001 – incorporated in Safe Port Act 2006
- Aim: encourage the supply chain parties themselves to improve security, reward with benefits
- Voluntary – to include importers, custom brokers, forwarders, carriers, logistics providers, and manufacturers
- Process
  - Sign agreement with CBP to cooperate, assess and improve security
  - Self assessment by applicant against security guidelines
  - Application (file Security Profile)

## CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

- Tier 1 – Certification after background investigation and document review of applicant
- Tier 2 – Validation after on site assessment (including foreign locations)
- Tier 3 – Compliance with additional guidelines
  - Periodic re- assessment and revalidation (every 4 years)
- Currently over 10,000 participants almost 5,500 of which have been validated at Tier 2

## CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM (C-TPAT)

- Benefits given by US Customs to C-PAT participants:
- Tier 1 (Certified Participants)
  - Reduced Risk Score in A.T.S. risk score and examination of cargo
  - Access to 'FAST' lanes on certain borders
- Tier 2 (Validated participants)
  - Further reduction in A.T.S risk score and examinations of cargo
  - Priority searches
- Tier 3 – (Participants complying with additional guidelines – 'Gold Standard')
  - Further reduction of the A.T.S score and examination of cargo
  - Priority for examinations
  - Expedited release during all threat levels

## CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM

- Effects on other countries
- C-TPAT companies increasingly contractually require foreign suppliers to meet C-TPAT security guidelines
- Participation in C-TPAT by foreign manufacturers is increasing i.e. in E.U. introduction of AEO
- C-TPAT companies first to be able to resume trade after security incident
- MRAs envisages avoiding duplication of efforts in other countries with similar customs trade partnerships arrangements

## SECURE FREIGHT INITIATIVE

- SECURE FREIGHT INITIATIVE (SFI) called for by the Safe Port Act of 2006
- Combines use of container Imaging and Radiation detection equipment
- Testing of feasibility of 100% container scanning at least 3 foreign ports to be followed by evaluation of pilots at these ports
- However 9/11 Commission Recommendations Act 2007 now demands
  - 100% scanning of US bound maritime containers at foreign ports by 1.7.2012

## 100% Container Scanning?

- ❑ This was highly controversial inside and outside US – Why?
  - ❑ Cost of equipment for ports
  - ❑ Risk of port congestion and delays to customers
  - ❑ Unclear who will scan and what will happen with the data (data overload)
  - ❑ Jurisdiction – US Cannot force other countries
  - ❑ Sufficient measures already in place
  - ❑ No reciprocity by US for their outbound cargo
- ❑ Safe Ports Re-Authorisation Act 2010 has now moved back target date from 2012 to 2014 given recognition that is not achievable in present economic climate if ever? It has also recommended in the amendment that such screening should be on a Risk Based Assessment. It also amends requirement in original act for all Containers to be both Scanned and Searched, now Scanned or Searched, dependant on risk assessment.

## EU Regulation No 648/2005 Community Customs Code

The above regulation now lays down the rules for the customs treatment of goods that are imported or to be exported.

It establishes an equivalent level of protection in customs controls for goods brought into or out of the customs territory of the Community.

It considers the need for a Community-wide risk management framework to support a common approach.

It requires setting priorities effectively and resources are allocated efficiently with the aim of maintaining a proper balance between customs controls and the facilitation of legitimate trade.

It endorses a framework to provide a common criteria and harmonised requirement for authorised economic operators and ensure a harmonised application of such criteria and requirements.

© LAIRDSIDE MARITIME CENTRE

## AUTHORISED ECONOMIC OPERATOR (European Accreditation)

- ❑ APPLICATION FOR AEO STATUS IS VOLUNTARY AND COMMENCED IN 2008. The scheme is now under World Customs Organisation Safe Framework of Trade, being rolled out worldwide 33 countries having introduced/about to introduce this scheme.
- ❑ Assessment process will decide what certification you receive:
- ❑ SECURITY AND SAFETY – Criteria: Customs compliance, Record Keeping, Financial solvency and appropriate Security and Safety measures.
- ❑ CUSTOMS SIMPLIFICATION – Criteria: Customs compliance, Record Keeping and Financial Solvency
- ❑ CUSTOMS SIMPLIFICATIONS/SECURITY AND SAFETY – Criteria: Customs compliance, Record keeping, Financial Solvency, Security and Safety and Security – and who wants to receive the benefits of both types of AEO.

© LAIRDSIDE MARITIME CENTRE

## AUTHORISED ECONOMIC OPERATOR

- ❑ SAFETY AND SECURITY CRITERIA FOR COMPLIANCE:
- ❑ ASSESSMENT COMPLETED ON FOLLOWING CRITERIA:
- ❑ SECURE PERIMETERS OF BUSINESS, ACCESS CONTROL MEASURES IN PLACE, AND MEANS OF DEALING WITH UNAUTHORISED ACCESS.
- ❑ MEASURES TO PROTECT CARGO UNITS
- ❑ MEASURES TO PREVENT UNAUTHORISED ACCESS TO SHIPPING AREAS, LOADING DOCKS AND CARGO AREAS BOTH ON ARRIVAL AND DISPATCH
- ❑ IN U.K. - PORTS WHICH ARE ISPS COMPLIANT WILL AUTOMATICALLY FULFIL THE ABOVE CRITERIA

© LAIRDSIDE MARITIME CENTRE

## AUTHORISED ECONOMIC OPERATOR

- ❑ SAFETY/SECURITY MEASURES IN PLACE FOR GOODS IN STORAGE OR MANUFACTURE
- ❑ MEASURES IN PLACE FOR SAFETY AND SECURITY OF GOODS IN TRANSIT INCLUDING THIRD PARTY TRANSPORT
- ❑ SAFETY AND SECURITY MEASURES AGREED WITH SUPPLIERS
- ❑ SCREENING OF EMPLOYEES IN SECURITY SENSITIVE LOCATIONS AND CONTRACTED PERSONNEL
- ❑ SAFETY AND SECURITY TRAINING FOR STAFF
- ❑ THIS IS A MORE PRAGMATIC APPROACH WHEN COMPARED WITH CSI.

© LAIRDSIDE MARITIME CENTRE

## AUTHORISED ECONOMIC OPERATOR

- ❑ BENEFITS FROM ACCREDITATION:
  - LOWER RISK SCORE FOR CUSTOMS RISK MANAGEMENT SYSTEMS – LOWERS FREQUENCY OF PHYSICAL AND DOCUMENTARY CHECKS
  - CONSIGNMENTS MAY BE FAST TRACKED THROUGH CUSTOMS CONTROLS. IF SELECTED FOR EXAMINATION WILL RECEIVE PRIORITY OVER NON AEO CARGO
  - RECOGNISED STATUS ACROSS E.U.
  - AN INDUSTRY KITE MARK AND USEFUL MARKETING TOOL
  - POTENTIAL FOR RECIPROCAL ARRANGEMENT AND MUTUAL RECOGNITION WITH COUNTRIES OUTSIDE E.U.

© LAIRDSIDE MARITIME CENTRE



## QUESTIONS?

© LAIRDSIDE MARITIME CENTRE

## LECTURE 14 TRAINING REQUIREMENTS

© LAIRDSIDE MARITIME CENTRE

### SECURITY TRAINING SHIPS - Requirements

Section 13.1  
IN RESPECT OF SHIP SECURITY, THE C.S.O. SHALL HAVE KNOWLEDGE OF AND RECEIVED ISPS TRAINING. MANDATORY IN UK

Section 13.1 & 2

IN RESPECT OF SHIP SECURITY, THE S.S.O. SHALL HAVE KNOWLEDGE OF AND RECEIVED ISPS TRAINING. MANDATORY IN UK

Section 13.3  
ALL OTHER SHIPBOARD PERSONNEL HAVING SPECIFIC SECURITY DUTIES SHOULD HAVE KNOWLEDGE AND RECEIVE TRAINING AS APPROPRIATE.

Section 13.4  
ALL OTHER SHIPBOARD PERSONNEL SHOULD HAVE KNOWLEDGE OF AND BE FAMILIAR WITH RELEVANT PROVISIONS OF THE SSP AS APPROPRIATE.

© LAIRDSIDE MARITIME CENTRE

### STCW78 As Amended – Manila 2010

- ❑ Amendments come into force from 1/1/2012
- ❑ SSO Training remains unchanged. Certificates should identify *“STCW '78, as amended, Regulation VI/5 and STCW Code Section A-VI/5”*
- ❑ Three new levels of training introduced for ISPS Compliant vessels. May also have extensions in flag states.
- ❑ Covered by Regulation VI/6, Section A-VI/6 (Annex 2) and Guidance given in Section B-VI/6 Annex 3.
- ❑ Security Familiarisation Training - All Crew
- ❑ Proficiency in Security awareness – All Crew
- ❑ Proficiency in Security Duties.

© LAIRDSIDE MARITIME CENTRE

### MSC/Circ.1235 21<sup>st</sup> Oct 2007

#### ❑ GUIDELINES ON SECURITY-RELATED TRAINING AND FAMILIARIZATION FOR SHIPBOARD PERSONNEL

##### 2 GENERAL PRINCIPLES

- 2.1 Shipboard personnel are not security experts and it is not the aim of the provisions of the Guidance to convert them into security specialists.
- 2.2 Shipboard personnel should receive adequate security-related training or instruction and familiarization training so as to acquire the required knowledge and understanding to perform their assigned duties and to contribute collectively to the enhancement of maritime security.
- 2.3 Shipboard personnel should receive adequate security-related training or instruction at least one time in their career.
- 2.4 The security-related familiarization training should be conducted by the ship security officer or an equally qualified person.

© LAIRDSIDE MARITIME CENTRE

### MSC/Circ.1154 T2/4.2 23 May 2005

#### ❑ GUIDELINES ON TRAINING AND CERTIFICATION FOR COMPANY SECURITY OFFICERS

© LAIRDSIDE MARITIME CENTRE

## SECURITY TRAINING PORTS Requirements

Similar requirements exist for Port Facilities

Section 18.1 & 18.2

IN RESPECT OF THE PORT FACILITY THE P F S O, SHALL HAVE KNOWLEDGE OF AND RECEIVED ISPS TRAINING, MANDATORY IN U.K.

Section 18.2

ALL OTHER PERSONNEL HAVING SPECIFIC SECURITY DUTIES SHOULD HAVE KNOWLEDGE AND RECEIVE TRAINING AS APPROPRIATE.

Section 18.3

ALL OTHER PERSONNEL SHOULD HAVE KNOWLEDGE OF AND BE FAMILIAR WITH RELEVANT PROVISIONS OF THE SSP AS APPROPRIATE

© LAIRDSE MARITIME CENTRE

## Developing Courses IMO Model Courses

- ❑ IMO Model Courses
- ❑ 3.19 SSO
  - 14 hours over 2 days
- ❑ 3.20 CSO
  - 18 hours over 3 days
- ❑ 3.21 PFSO
  - 18 hours over 3 days
- Minimum requirements
- Provides guidance to training establishments.
- Not a rigid format.
- Each state to provide own structures and as necessary approvals.

© LAIRDSE MARITIME CENTRE

## Training Level and Content

- ❑ Must be practical
- ❑ Provide proportionate knowledge of the environments likely to be encountered
- ❑ Emphasise the Ship-Port and Ship-Ship Interface requirements
- ❑ Develop a Risk Assessment methodology throughout
- ❑ Emphasise the importance of Communication throughout
- ❑ PROPORTIONATE, PRAGMATIC

© LAIRDSE MARITIME CENTRE

## EU Approved Training - 1

- ❑ UK through MCA/MNTB have own requirements.
- ❑ Where the basis for the development of IMO Models.
- ❑ UK training is approved by
  - MCA – Ship & Company Security Officers
  - TRANSEC – Port Facility Security Officers
- ❑ Training Providers approved and courses verified and audited

© LAIRDSE MARITIME CENTRE

## UK APPROVED TRAINING COURSES 2

- ❑ In UK the following must attend an approved training Course before taking up role
  - Ships Security Officer (3 Days)
  - Company Security Officer (4 Days)

Both accredited by the Maritime Coastguard Agency (MCA)

© LAIRDSE MARITIME CENTRE

## CONTRACTING GOVERNMENT TRAINING REQUIREMENTS - SHIPS

- ❑ FOR UK SHIPS ALL CREW MUST DEMONSTRATE SUFFICIENT KNOWLEDGE TO PERFORM THEIR SECURITY DUTIES IN RESPECT OF THE SHIPS SECURITY PLAN. CURRENTLY THERE IS NO MANDATED TRAINING REQUIRED.
- ❑ FROM 1.1.08 SSO TRAINING WAS BROUGHT INTO THE STCW CODE THROUGH IMO RESOLUTIONS MSC. 203 (81) AND MSC. 209(81).
- ❑ FROM THIS DATE ALL SSO TRAINING MUST ASSESS THE COMPETENCIES STATED IN CHAPTER A - VI TABLE A -VI/5 ' SPECIFICATIONS OF MINIMUM STANDARDS OF THE PROFICIENCY FOR SECURITY OFFICERS'
- ❑ PRIOR TRAINING TO THE IMO MODEL COURSE MET THIS NEW SPECIFICATION

© LAIRDSE MARITIME CENTRE

## STCW Manila Amendments 2010

- ❑ Come into force 1/1/2012
- ❑ Certificate of Proficiency in Security Awareness
- ❑ Certificate of Proficiency in Security Duties
- ❑ MEMBER STATES PROVISIONS?????

© LAIRDSIDE MARITIME CENTRE

## EUROPEAN METHODS



© LAIRDSIDE MARITIME CENTRE

## How can this be achieved?

- ❑ Ideally on board
  - Mentoring
  - Personal commitment/CPD
  - Familiarisation - Should be part of ISM
- ❑ Are ships staff suitably trained in training methods?

© LAIRDSIDE MARITIME CENTRE

## Regulation STCW A1/6

- ❑ TRAINING & ASSESSMENT
- ❑ ....2. those responsible for training and assessment of competence of seafarers, as required under the convention, are appropriately qualified in accordance with the provisions of section A-1/6 of the STCW Code for the type and level of training or assessment involved.

© LAIRDSIDE MARITIME CENTRE

## STCW A1/6 Training & Assessment

Any person conducting in service training shall have:

- ❑ Appreciation of training programme
- ❑ Be qualified for the task

Any person conducting in service assessment shall

- ❑ Have an appropriate level of knowledge and understanding of the competence to be assessed
- ❑ Be qualified for the task
- ❑ Have received appropriate guidance in assessment methods and practice

- ❑ However STW38/WP.3 has considered that this requirement would not be necessary for SSO's providing on board familiarisation training

© LAIRDSIDE MARITIME CENTRE

## Qualification requirements for trainers and assessors

- ❑ Should be meeting the requirements of STCW B1/6
  - Received appropriate guidance in assessment methods and practice
  - Gained practical assessment experience under the supervision and to the satisfaction of an experienced assessor
  - A full understanding of training methods and practice

© LAIRDSIDE MARITIME CENTRE

## IMO Model Course 6.09

- ❑ TRAINING FOR INSTRUCTORS
- ❑ 5 day programme
  - Teaching methods
  - Presentation techniques
  - Course preparation methods
  - Assessment methods
- ❑ Practical Course

© LAIRDSIDE MARITIME CENTRE

## TRAINING – THE MASTER

Although there is no specific requirement under the ISPS for the Master to undergo accredited training

As the Master is a signatory to the Declaration of Security and having ultimate responsibility for the ship's safety should be adequately trained in his responsibilities. But... and ISPS A13.3 in association with

- ❑ MSC1235:2007 which identifies....
  - 1.2 The term "shipboard personnel" means:  
The master and the members of the crew or other persons employed or engaged in any capacity on board a ship on the business of that ship.... IMPLIES THAT THE MASTER WILL HAVE THE APPROPRIATE KNOWLEDGE

© LAIRDSIDE MARITIME CENTRE

## SECURITY STAFF – UK GOVERNMENT REQUIREMENTS

- ❑ ALL CONTRACT SECURITY STAFF IN U.K. HAVE TO BE LICENSED WITH GOVERNMENT BODY 'SECURITY INDUSTRY AUTHORITY' TO CARRY OUT ROLES AS:
  - ❑ STATIC GUARD
  - ❑ RETAIL GUARD
  - ❑ WHEEL CLAMPING OPERATIVE
  - ❑ DOORMEN
- ❑ TO BE LICENSED MUST RECEIVE ACCREDITED TRAINING AND PASS EXAMINATIONS IN BOTH PRACTICAL KNOWLEDGE AND CONFLICT MANAGEMENT SKILLS
- ❑ CRIMINAL RECORD CHECKS COMPLETED
- ❑ ON APPLICATION AND APPROVAL OF LICENCE, DETAILS AND PHOTOGRAPHIC I.D. PLACED ON GOVERNMENT BODY'S DATA BASE.
- ❑ OFFENCE IN UK TO CARRY OUT SUCH ROLES WITHOUT LICENCE

© LAIRDSIDE MARITIME CENTRE

## U.K. GOVERNMENT TRAINING REQUIREMENTS

- ❑ ADDITIONALLY SECURITY STAFF EMPLOYED ON PORTS MUST RECEIVE TRAINING WHICH COVERS THE REQUIREMENTS OF Part 'B' Para18.2
- ❑ THIS CONSISTS OF 16 MODULES WHICH INCLUDE:
  - ❑ The Threat to Maritime Environment
  - ❑ Objectives and Organisation of Maritime Security
  - ❑ Security Communications within the Port
  - ❑ Response to/Reporting of Security Incidents
  - ❑ Legal Powers of Security Staff
  - ❑ Dealing with Aggression
  - ❑ Restricted area access control/patrolling
  - ❑ Recognition of Firearms, explosives, incendiary devices
  - ❑ Searching People, Vehicles, baggage, Freight and Cargo
  - ❑ Handling of Telephoned Bomb Warning

© LAIRDSIDE MARITIME CENTRE

## CONTRACTING GOVERNMENT TRAINING REQUIREMENTS - PORTS

- ❑ ALL OTHER STAFF ON PORTS SHOULD RECEIVE THE REQUIRED TRAINING UNDER Part 'B' 18.3. (TRANSEC) SECURITY WING OF DEPARTMENT OF TRANSPORT IN U.K. HAVE PRODUCED D.V.D. TO FULFIL THIS TRAINING ELEMENT.

© LAIRDSIDE MARITIME CENTRE

## SEARCH TECHNIQUES TRAINING Part 'B' 13.3 & 18.2

- ❑ Particularly important that crew/port staff with search responsibilities have training in search techniques
- ❑ Training should encompass searching:-
  - People
  - Bags
  - All vehicles
  - Use of equipment – AMD, HHMD, X RAY, AND EXPLOSIVE IDENTIFICATION
- ❑ Staff should be recognise weapons and devices
- ❑ Refresher training to be undertaken on a regular basis

© LAIRDSIDE MARITIME CENTRE

## U.K. BOMB THREAT ASSESSMENT TRAINING

- ❑ Requirement to distinguish between credible and non-credible bomb threats
- ❑ Port Facility must ensure sufficient staff receive training in bomb threat assessment
- ❑ At least one person so trained should be available at all times

© LAIRDSIDE MARITIME CENTRE

## Qualification & Training of Duly Authorised Officers

- ❑ MSC Circ 1111/2004 gives guidance on the qualifications and training of Duly Authorised Officers
- ❑ appropriate knowledge of the provisions of chapter XI-2 and of the ISPS Code, of shipboard operations and need to be appropriately qualified and trained to the level required by the functions that they are authorized to carry out.
- ❑ Communicate in English
- ❑ periodically undergo training in order to update their knowledge.

© LAIRDSIDE MARITIME CENTRE

## INSTRUCTIONAL TECHNIQUES 1

Information can be passed on by:

- ❑ CASE STUDIES
- ❑ PRACTICAL HANDS ON APPLICATION
- ❑ MENTORING
- ❑ GROUP EXERCISES & DISCUSSION
- ❑ AUDIO VISUAL MATERIALS

© LAIRDSIDE MARITIME CENTRE

## Methods & Media

- ❑ Training should be developed on the Learning Styles
- ❑ Everyone has preferences for the way in which they learn:
  - Activists – Concrete Experience
  - Pragmatists – Active Experimentation
  - Reflectors – Reflective Observation
  - Theorists – Abstract Conceptualisation
- ❑ Exercises
- ❑ AV Aids

© LAIRDSIDE MARITIME CENTRE

## TRAINING VALUE ?



© LAIRDSIDE MARITIME CENTRE

## Questions?

© LAIRDSIDE MARITIME CENTRE

## LUNCH

© LAIRDSIDE MARITIME CENTRE

## Lecture 15 "Drills, Exercises"

© LAIRDSIDE MARITIME CENTRE

### DRILLS AND EXERCISES

- ❑ 13.3. Part A
- ❑ Shipboard personnel having specific security duties and responsibilities for ship security as described in the ship security plan, shall have sufficient knowledge and ability to perform their assigned duties.
- ❑ HOW DO YOU TEST THIS?

© LAIRDSIDE MARITIME CENTRE

### SECURITY DRILLS & EXERCISES

- ❑ Section 13.4, Part A
- ❑ To ensure the effective implementation of the Ships Security Plan, drills should be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances, taking into account the guidance given in Part B of this Code.
- ❑ Section 13.5 Part A
- ❑ Company Security Officer should ensure that effective co-ordination and implementation of Ships Security Plans by participating in exercises at appropriate intervals
- ❑ MANDATORY THROUGHOUT E.U. UNDER REGULATION E.U. 725/2004

© LAIRDSIDE MARITIME CENTRE

### INTERPRETATION – Drill & Exercise?

- ❑ FINLAND - 13.6 ja 13.7 (alusten miehistön sekäyhtiön turvapaallikoiden ja alusten turvapaallikoiden turvajarjoitusten tiheys).
- ❑ GERMANY - 13.6. und 13.7. (Häufigkeit von Schulungen und Übungen zur gefahrenabwehr für Schiffsbesatzungen sowie für die Beauftragten für die Gefahrenabwehr im Unternehmen und auf dem Schiff).
- ❑ SWEDEN 13.6 och 13.7 (periodicitet i fråga om utbildningar och övningar med avseende på sjöfartsskydd för fartygens besättningar och för rederiernas och fartygens skyddschefer).

© LAIRDSIDE MARITIME CENTRE

### Drills & Exercises

- ❑ What is a Drill ?
  - What does it test?
- ❑ What is an Exercise?
  - What does it test?

© LAIRDSIDE MARITIME CENTRE

## SECURITY DRILLS & EXERCISES 1

- ❑ SECURITY DRILLS SHOULD BE CARRIED OUT EVERY:
  - PORT – 3Months
  - SHIP – 3 Months / 25% CREW CHANGE
- ❑ SECURITY EXERCISES SHOULD BE CARRIED OUT EVERY:
  - PORT & SHIPS 1 Calendar Year (No more than 18 months between )

In U.K. under Ship and Port Facility (Security) Regulations 2004. Failure to carry out and record such Drills and Exercises, can result in Enforcement Notice served on SSO Failure to conform to such Notice may result in Court appearance and Fine. Continue failure after conviction can result in £100 per day fine until conforming to Enforcement Notice.

© LAIRDSIDE MARITIME CENTRE

## SECURITY DRILLS

- ❑ Examples
  - Carrying out an Evacuation
  - Requiring a Pass Issuing Officer to detail the procedure to be followed in the loss of a Pass
  - Replicate a Bomb Threat with Staff using a Bomb Threat Check List
  - Responding to breaches of Access to R.A/Controlled Buildings
  - Requiring Security Staff to detail procedures for identification of suspicious vehicles
  - Responses to Discovery of weapons
- ❑ It is essential that Drills test that Staff can respond effectively to increases in Security level, particularly those only activated at Level 2

© LAIRDSIDE MARITIME CENTRE

## SECURITY EXERCISES Section 13.7 Part B / 18.6 Part B

Various types of exercises which may include participation of port facility security officers, in conjunction with relevant authorities of Contracting Governments, Company Security officers, or Ship Security Officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. Requests for the participation of company security officers or ships security officers in joint exercises should be made bearing in mind the security and work implications for the ship. These exercises should test communication, coordination, resource availability and response.

These exercises may be:

- 1 full scale or live;
- 2 tabletop simulation or seminar; or
- 3 combined with other exercises held such as emergency response or other port

© LAIRDSIDE MARITIME CENTRE

## SECURITY EXERCISES

- ❑ SOME EXAMPLES MAY INCLUDE:
  - DAMAGE TO DESTRUCTION OF PORT FACILITY
  - HIJACKING OR SEIZURE OF SHIP
  - TAMPERING WITH CARGO/STORES
  - UNAUTHORISED ACCESS INCLUDING STOWAWAYS
  - SMUGGLING WEAPONS/EXPLOSIVES
  - USE OF SHIP AS A WEAPON
  - BLOCKADING OF A PORT FACILITY
  - NUCLEAR, BIOLOGICAL OR CHEMICAL ATTACK

© LAIRDSIDE MARITIME CENTRE

## ASSESSMENT OF DRILLS AND EXERCISES

- HAVING CONDUCTED A DRILL IT IS ESSENTIAL TO REVIEW, EVALUATE AND ASSESS THE OUTCOME WITH A VIEW TO IMPROVE THE SYSTEM AND THE PFSP/SSP
- ALL DRILLS AND EXERCISES SHOULD BE RECORDED AND KEPT FOR THE MINIMUM PERIOD AS SPECIFIED BY THE ADMINISTRATION.
- MAY BE RECORDED IN ELECTRONIC FORMAT, BUT PROTECTED AGAINST UNAUTHORISED DELETION, DESTRUCTION OR AMENDMENT.

© LAIRDSIDE MARITIME CENTRE

## SECURITY LEVELS BEST PRACTICE

- ❑ Ship and Port facility staff with security responsibilities must be adequately drilled to ensure that they can respond effectively to increases in Security Levels.
- ❑ Special importance for crew and staff members activated for purposes at Security Level 2
- ❑ There should be one hypothetical Security Level amendment per year

© LAIRDSIDE MARITIME CENTRE



## SOME EXERCISES CONDUCTED

- ❑ LARNE - NORTHERN IRELAND
- ❑ HEYSHAM - LANCASHIRE
- ❑ P&O - PORT OF LIVERPOOL
- ❑ JERSEY - PORT OF JERSEY
- ❑ IoM SEACAT - LIVERPOOL

© LAIRDSIDE MARITIME CENTRE

## PORT OF LIVERPOOL MAY 2005

- ❑ Seminar based
- ❑ 2005 - PFSO'S
- ❑ 2007 - OBC'S



© LAIRDSIDE MARITIME CENTRE

## MULTI AGENCY EXERCISES

© LAIRDSIDE MARITIME CENTRE

BIOLOGICAL/CHEMICAL/NUCLEAR



CHEMICAL/BIOLOGICAL/NUCLEAR



BIOLOGICAL/CHEMICAL / NUCLEAR



## OPERATIONAL ISSUES

- ❑ Securing Area
- ❑ Control of Public
- ❑ Logistics
- ❑ Catering
- ❑ Toilet Facilities
- ❑ Rest and Welfare
- ❑ Observers
- ❑ Health and Safety



© LAIRDSIDE MARITIME CENTRE

## LATVIA 15-16 May, 2007

- ❑ Operation Bold Mercy
- ❑ Major Inter department, multi national exercise.
- ❑ Hijack of Passenger Ferry in Baltic and subsequent explosion with many casualties.
- ❑ 12 months in planning



© LAIRDSIDE MARITIME CENTRE

## Turkey

- ❑ Turkey Multi Department Exercise "Tatbikati" 2008 & 2009
- ❑ Bartın Limanı'nda ISPS Tatbikati yapıldı
- ❑ Other Member States????



Questions ?

© LAIRDSIDE MARITIME CENTRE

## Lecture 16 "Security Administration"

© LAIRDSIDE MARITIME CENTRE

## Documentation Records Section 10.1 Part A

THESE SHALL INCLUDE:

- ❑ TRAINING, DRILLS & EXERCISES
- ❑ SECURITY THREATS AND INCIDENTS
- ❑ BREACHES OF SECURITY
- ❑ CHANGES IN SECURITY LEVELS
- ❑ SECURITY RELATED COMMUNICATIONS
- ❑ INTERNAL SECURITY AUDITS
- ❑ PERIODIC REVIEW OF SSA and SSP
- ❑ IMPLEMENTATION OF AMENDMENTS TO SSP
- ❑ SECURITY EQUIPMENT MAINTENANCE RECORDS
- ❑ TESTING SHIP SECURITY ALERT SYSTEM

REQUIRED FOR INSPECTION UNDER MSC/CIRC.1151

© LAIRDSIDE MARITIME CENTRE

## RECORDING OF SECURITY THREATS & INCIDENTS

### Section 10.1.2 Part A

TYPICAL INCIDENTS MAY BE SUCH AS:-

- ❑ FIRE ON BOARD THROUGH ARSON
- ❑ BOMB THREAT
- ❑ EVIDENCE OF ATTEMPTED ENTRY TO RESTRICTED AREAS ON BOARD
- ❑ STOWAWAYS ON LORRIES/VESSEL
- ❑ UNAUTHORISED PERSONNEL ON BOARD VESSEL
- ❑ SUSPECT PERSONAL DOCUMENTATION
- ❑ PORT SECURITY INCIDENTS

© LAIRDSIDE MARITIME CENTRE

## CERTIFICATION Part A Section 19

- ❑ SSA and SSP submitted
- ❑ Initial verification
  - Systems
  - Equipment
  - Application of SOLAS XI-2 and ISPS Part A
- ❑ International Ship Security Certificate (ISSC) Issued after verification/renewal
- ❑ Valid for a period not exceeding 5 years (5 yr in UK)
- ❑ Intermediate verifications (at least 1) to ensure compliance between 2<sup>nd</sup> & 3<sup>rd</sup> anniversary
- ❑ Renewal verification not exceeding 5 years

© LAIRDSIDE MARITIME CENTRE

## INTERIM CERTIFICATION Part A Section 19.4

- ❑ After 1/7/04 *Interim Certificates may be issued for:-*
  1. a ship without a certificate, on delivery or prior to its entry or re-entry into service;
  2. transfer of a ship from the flag of a Contracting Government to the flag of another Contracting Government;
  3. transfer of a ship to the flag of a Contracting Government from a State which is not a Contracting Government; or
  4. when a Company assumes the responsibility for the operation of a ship not previously operated by that Company;

© LAIRDSIDE MARITIME CENTRE

## CERTIFICATION ISSUES



- ❑ New Builds will not be issued ISSC whilst under construction.
- ❑ Ship Conversions
  - Long Process
  - Skeleton manning
  - No SSO ? – ISSC requirements invalidated
  - Once converted new SSP required
- ❑ Repair, in scope of Code and all measures maintained.

© LAIRDSIDE MARITIME CENTRE

## REVIEW OF THE SSP

As we have seen;

- ❑ A SSP review should be taken regularly and MUST be reviewed when;
- ❑ The relevance of the SSP has been affected by Operational Changes

© LAIRDSIDE MARITIME CENTRE

## REPORTING DEFFICIENCIES

### Section 12.2.5 PART A

- ❑ THE SSO IS RESPONSIBLE FOR REPORTING TO THE CSO ANY DEFFICIENCIES AND NON-CONFORMITIES IDENTIFIED DURING AUDIT, REVIEW AND
- ❑ INSPECTION VERIFICATIONS OF COMPLIANCE AND IMPLEMENTING CORRECTIVE ACTIONS

### Section 11.2.7 PART A

- ❑ "THE CSO SHALL ENSURE THESE ISSUES ARE PROMPTLY ADDRESSED AND DEALT WITH".

© LAIRDSIDE MARITIME CENTRE

## SECURITY INCIDENT REPORTING

- ❑ Systems are required to cover two aspects of Security Incident Reporting:
  - Port Facility Personnel to report Security incidents at the facility (INTERNAL REPORTING)
  - SSO's and CSO's to Report Security Incidents to Contracting Governments as detailed in the SSP (EXTERNAL REPORTING).
  - For example in the UK TRANSEC collate Security Reports

© LAIRDSIDE MARITIME CENTRE

## OBLIGATIONS FOR REPORTING SECURITY INCIDENTS

- ❑ FOR EACH CONTRACTING GOVERNMENT WHERE IS THIS RESPONSIBILITY PLACED?

© LAIRDSIDE MARITIME CENTRE

## Ship and Port Facility Security Regulations

Contracting Governments should provide:-

- ❑ Reporting Requirements
- ❑ TRANSEC Maritime Security Circular No.1/01. Under ISPS, the requirements are very similar
- ❑ Responsibility:
  - Ship owners, Charterers, Managers or Masters
  - Harbour Authorities
  - Harbour Operators
  - Persons carrying on operations in a Harbour area
- ❑ Includes UK Passenger ship operations overseas

© LAIRDSIDE MARITIME CENTRE

## RESTRICTED AREA IDENTIFICATION

- ❑ EU Regulation "Enhancing Ship and Port Facility Security" provides the mechanism to declare restricted areas. Any such areas should be suitably identified.
- ❑ Signs for:-
  - ❑ RESTRICTED AREA PERIMETERS
  - ❑ RESTRICTED AREA ACCESS AND SEARCH POINTS

© LAIRDSIDE MARITIME CENTRE

## APPROPRIATE WORDING

- ❑ Search areas:

Searches:

In the interest of public safety and security under regulation (EC) Reg. No. 725/2004 on Enhancing Ship and Port Security you may be required to submit yourself, your baggage and your vehicle to search prior to entry into this Restricted Area.

© LAIRDSIDE MARITIME CENTRE

## CCTV - PERSONAL PRIVACY - HUMAN RIGHTS

UK POSITION

- ❑ DATA PROTECTION ACT
- ❑ CCTV Data captured and recorded must be treated in accordance with the DPA.
- ❑ Personal data must be:
  - Fairly and lawfully possessed
  - Processed for limited purposes and not in a manner incompatible with those purposes
  - Adequate, relevant and not excessive
  - Accurate
  - Kept no longer than necessary
  - Processed in accordance with individual rights
  - Secure
  - Not transferred to unauthorised bodies without adequate protection

www.dataprotection.gov.uk

© LAIRDSIDE MARITIME CENTRE

## REPORTING METHODOLOGY?

- ❑ Incidents of which the Media are aware
- ❑ Bomb warnings
- ❑ Hijack
- ❑ Discovery of Firearms and ammunition
- ❑ Discovery of Other weapons
- ❑ Discovery of explosives
- ❑ Unauthorised access to restricted areas
- ❑ Miscellaneous Incidents
  
- ❑ ARE THESE APPROPRIATE FOR GOVERNMENT?

© LAIRDSIDE MARITIME CENTRE

## MEDIA IMPACT

Power depends on public opinion.

It is mass media that shapes public opinion.

Mass media is willing to cover sensations.

That's why today the most effective method of terror is psychological attack.

*Psychological attack is violence not against the representatives of power, but directed against peaceful, unprotected citizens. It is always accompanied by the demonstration through the mass media of the results of terror.*

1-8-2000

## TRANSEC Reporting

Incident Type	Immediate	1 Month
Incidents of which Media aware	X	
Bomb Warnings Credible	X	
Bomb Warnings Non Credible		X
Hijack	X	
Discovery of Firearms/Ammunition Suspicious	X	
Discovery of Firearms/Ammunition Routine		X
Discovery of other weapons Suspicious	X	
Discovery of other weapons Routine		X
Discovery of Explosives Suspicious	X	
Discovery of Explosives Routine		X
Unauthorised Access to Restricted areas - Suspicious	X	
Unauthorised Access to Restricted areas - Routine		X
Miscellaneous Incidents	As considered appropriate	

© LAIRDSIDE MARITIME CENTRE

## Reporting to Flag States

- ❑ MSC Circ 1133/2004 REMINDS ADMINISTRATIONS OF THE OBLIGATION TO NOTIFY FLAG STATES AND IMO OF ALL COMPLAINTS STEPS TAKEN AGAINST SHIPS WHEN EXERCISING CONTROL AND COMPLIANCE MEASURES IN REGARD TO SOLAS XI-2/9

© LAIRDSIDE MARITIME CENTRE

Questions?

© LAIRDSIDE MARITIME CENTRE

COFFEE

© LAIRDSIDE MARITIME CENTRE

## Exercise 5 – CERTIFICATION AND ADMINISTRATION

© LAIRDSIDE MARITIME CENTRE

## Lecture 17 AUDIT and REVIEW/VERIFICATION

© LAIRDSIDE MARITIME CENTRE

### REQUIREMENT FOR AUDIT

- ❑ A9.4.8 requires procedures for auditing the security activities. Ports (A16.3.13) similarly
- ❑ A9.4.1 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/Ship/Port Facility. (16.3.1 similarly)
- ❑ 10.1.6 & 10.1.7 Records of internal audits and reviews of security activities

© LAIRDSIDE MARITIME CENTRE

### Auditing

#### TWO LEVELS

1. Internal – Shipping Company requirements
2. External – 2<sup>nd</sup> and 3<sup>rd</sup> Party

© LAIRDSIDE MARITIME CENTRE

### Audit Types

- ❑ **Internal audits**, generally termed first-party audits, are conducted by, or on behalf of, the organization itself for management *review* and other internal purposes, and may form the basis for an organization's self-declaration of conformity.
- ❑ **External audits** generally termed second- and third-party audits.
  - Second-party audits are conducted by parties having an interest in the organization.
  - Third-party audits are conducted by external, independent auditing organizations.

© LAIRDSIDE MARITIME CENTRE

### What is Auditing?

- ❑ Various uses of the word.
- ❑ ISO9001:2008 Section 8:
- ❑ The Audit process **MUST** verify compliance with.....
- ❑ A systematic, independent and documented process for obtaining evidence and evaluating it objectively to determine the extent to which the required criteria are fulfilled.
- ❑ An Audit **MUST NOT** be confused with surveillance, inspection or review

© LAIRDSIDE MARITIME CENTRE

## Origin (Oxford Dictionary)

- ❑ late Middle English: origins from Greek *aud-* 'hear, listen'
- ❑ and Latin *auditus* 'hearing', from *audire* 'hear',
- ❑ in medieval Latin *auditus (compoti)* 'audit (of an account)', an audit originally being presented orally

© LAIRDSIDE MARITIME CENTRE

## Institute of Internal Auditors Definition

The Institute of Internal Auditors defines internal auditing as:

- ❑ '..... an independent, objective assurance and consulting activity designed to add value and improve an organisation's operations. It helps an organisation accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of risk management, control and governance processes.'

© LAIRDSIDE MARITIME CENTRE

## ISO19011:2005

- ❑ Auditing is characterized by reliance on a number of principles. These principles should help to make the audit an effective and reliable tool in support of management policies and controls by providing information on which an organization can act to improve its performance.
- ❑ Adherence to these principles is a prerequisite for providing audit conclusions that are relevant and sufficient and for enabling auditors working independently from one another to reach similar conclusions in similar circumstances.

© LAIRDSIDE MARITIME CENTRE

## ISO19011:2005

- ❑ **4.5.2 Consistency of auditors**
- ❑ Audits conducted by different auditors should arrive at similar conclusions when the same operation is audited under the same conditions.
- ❑ Audit programme management should establish methods to measure and compare auditor performance to achieve consistency among auditors.

© LAIRDSIDE MARITIME CENTRE

## Purpose of the Audit

- ❑ As well as ensuring that audit criteria are fulfilled, one purpose of an audit should evaluate the need for continual improvement
- ❑ Also an Audit should seek to confirm compliance NOT.... Seek to find Non Compliance
- ❑ It should verify that procedures are followed and requirements are met

© LAIRDSIDE MARITIME CENTRE

## What the Audit does

- ❑ Find objective evidence
- ❑ Look for compliance
- ❑ Identify any non conformance
- ❑ Assess suitability of the Security System
- ❑ Evaluate the effectiveness of any corrective actions

© LAIRDSIDE MARITIME CENTRE



## Why Audit?

- ❑ Find facts
- ❑ To gain objective evidence
- ❑ Demonstrate effectiveness of the system
- ❑ Demonstrate that requirements are met
- ❑ Identify the root cause of any deficiencies
- ❑ Ensure the system is up to date
- ❑ Verify compliance to Part A of ISPS Code/EU725:2004 and other National Legislation

© LAIRDSIDE MARITIME CENTRE

## RESPONSIBILITIES 1

### AS WE HAVE SEEN PREVIOUSLY

#### ❑CSO

- A11.2.5 arranging for internal audits and reviews of security activities;
- A11.2.7 ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;

#### ❑SSO

- A12.2.5 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;

© LAIRDSIDE MARITIME CENTRE

MSC.1/Circ.1217  
14 December 2006

### ❑ INTERIM GUIDANCE ON VOLUNTARY SELF-ASSESSMENT BY COMPANIES AND COMPANY SECURITY OFFICERS (CSOs) FOR SHIP SECURITY

- ❑ Provides guidance to assist Companies in the implementation of, and the maintenance of compliance with, the requirements of SOLAS chapter XI-2 and the ISPS Code.

© LAIRDSIDE MARITIME CENTRE

## RESPONSIBILITIES 2

- ❑ B1.2 The Port Facility Security Officer should implement the provisions of the PFSP and monitor the continuing effectiveness and relevance of the plan, including commissioning internal audits of the application of the plan.

© LAIRDSIDE MARITIME CENTRE

## AUDIT, REVIEW AND AMENDMENT

- ❑ 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.

- ❑ CONFUSING !!!!

© LAIRDSIDE MARITIME CENTRE

## REVIEW

Some additional definitions

### NOUN

- ❑ an inspection or examination by viewing, especially a formal inspection
- ❑ a second or repeated view of something
- ❑ a viewing of the past; contemplation or consideration of past events, circumstances, or facts.

### VERB

- ❑ to view, look at, or look over again.
- ❑ to inspect, especially formally or officially

© LAIRDSIDE MARITIME CENTRE

## REVIEW

- REVIEW - To examine again.

© LAIRDSIDE MARITIME CENTRE

## AUDIT versus REVIEW

SO in general principle,

- The Review seeks to establish that the system is Fit for purpose
- The Audit seeks to confirm that processes are being followed

The external Verification: in principle combines elements of review and audit to establish compliance AND to identify weaknesses in the system.

© LAIRDSIDE MARITIME CENTRE

## SECURITY AUDITS & INSPECTIONS

AUDITING AGAINST THE ISPS CODE IS IDENTICAL TO AUDITING AGAINST SIMILAR CODES SUCH AS:

- ISM CODE
- ISO QUALITY STANDARD 9001:2008
- ISO ENVIRONMENTAL STANDARD 14001
- ISO OH&S STANDARD 18001

*Internal auditors should be independent of the areas audited.*

*Ideally they should have some form of qualification in the practice.*

*IRCA approve a range of appropriate courses which provide skills in best practice.*

© LAIRDSIDE MARITIME CENTRE

## AUDITING PROCESS 1

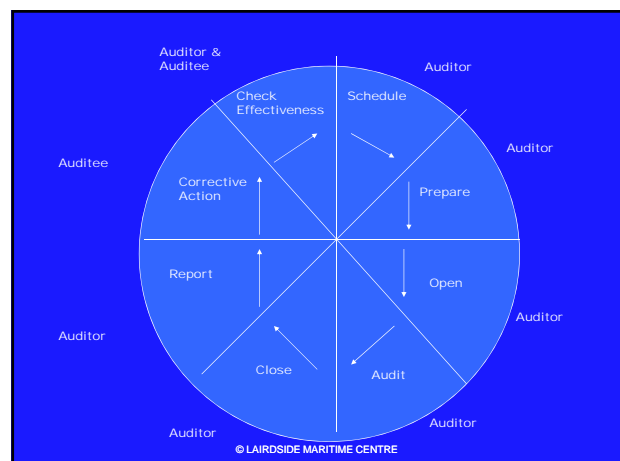
- Auditing should be undertaken against Documented procedures and the relevant SSP. As required by the Code the Auditing Process should measure conformance of operation against the stated procedures and the measures of the Security Plan and the requirements of Part A of the Code.
- Audits are required to be undertaken internally at least once per year
- An Auditor can ONLY Audit against the Code, the Legal requirements and what the Plan says, not what you think you would like to see.
- An "Observance" can be used to identify aspects "Best Practice" where considered necessary

© LAIRDSIDE MARITIME CENTRE

## AUDITING PROCESS 2

- Schedule
- Preparation
- Opening Meeting
- Audit
- Closing Meeting
- Reporting findings
- Develop Corrective Actions
- Check Effectiveness

© LAIRDSIDE MARITIME CENTRE



## Preparation for the Audit

- ❑ Confirm Date, Time and venue
- ❑ Obtain necessary documents
- ❑ Look for previous reports
- ❑ Ensure no outstanding issues
- ❑ Prepare a Check List

© LAIRDSIDE MARITIME CENTRE

## Checklists

- ❑ Guide for the Auditor
- ❑ Cover Scope of the Audit
- ❑ Plan
- ❑ Time Management
- ❑ Structured Process
- ❑ Not restrictive
- ❑ Allow for improved suggestions

© LAIRDSIDE MARITIME CENTRE

## Opening the Audit

- ❑ Formal or Informal?
- ❑ Confirm the Scope and the Schedule
- ❑ Explain the Reporting System
- ❑ Confirm Crew and Staff availability
- ❑ Confirm Confidentiality

© LAIRDSIDE MARITIME CENTRE

## Audit

- ❑ OBJECTIVE EVIDENCE
  - Interview
  - Observation
  - Records
  - Take Notes of Above

© LAIRDSIDE MARITIME CENTRE

## Closing the Audit

- ❑ Report Audit findings
- ❑ Identify non-conformances
- ❑ Re-confirm confidentiality
- ❑ Give positive feedback

© LAIRDSIDE MARITIME CENTRE

## Documented System

- ❑ ISPS Code (ISM Code)
- ❑ Ship Security Plan
- ❑ Annexed Plans
- ❑ Procedures
- ❑ Work Instructions and forms
- ❑ Records (Part 10 and others)

© LAIRDSIDE MARITIME CENTRE

## Auditing a Documented System

- ❑ Links between all levels of the system (Procedures, Forms, Log entries etc)
- ❑ Detail in Documents and Records
- ❑ Records to show the evidence
- ❑ Sample Records
- ❑ Sample a variety of areas

© LAIRDSIDE MARITIME CENTRE

## Conformance or non conformance???

- ❑ EU Reg. 324:2008
- ❑ Article 2
- ❑ ISO 9001:2008

© LAIRDSIDE MARITIME CENTRE

## Non- Conformance 1

- ❑ Not meeting the requirements of
  - SOLAS XI-2
  - Part A ISPS Code
  - EU Reg 725:2004
  - National Legislation
  - SSP
  - Company Procedures
  - Incomplete or no Records
  - Absence of objective evidence so as to demonstrate compliance

© LAIRDSIDE MARITIME CENTRE

## Non Conformance 2

- ❑ Clearly Understood
- ❑ Contain evidence of non conformance
- ❑ What is it against (Procedure, standard, activity, etc)
- ❑ Corrective action – implemented by Auditee
- ❑ Verified as completed by the Auditor

© LAIRDSIDE MARITIME CENTRE

## Audit Types

- ❑ Internal
- ❑ Second Party
- ❑ Third Party (External)
- ❑ Document Review
- ❑ Vertical Audit
- ❑ Process Audit

© LAIRDSIDE MARITIME CENTRE

## Audit Tools - QUESTIONS

- ❑ One question at a time
  - Where
  - What
  - When
  - How
  - Why
  - Who
  - Show me
  - First question
- ❑ OPEN COMMUNICATION METHOD
- ❑ CROSS QUESTIONING

© LAIRDSIDE MARITIME CENTRE

## Audit Tools - METHOD

- ❑ Audit in both Directions
- ❑ Read Documents
- ❑ Observe the situation
- ❑ Listen
- ❑ Keep Notes
- ❑ Give People time
- ❑ Non verbal communication
- ❑ Talk to the right people
- ❑ FIND OBJECTIVE EVIDENCE

© LAIRDSIDE MARITIME CENTRE

## Audit Tools – MANGING TIME

- ❑ Planning
- ❑ Taking Notes
- ❑ Do not waste time with
  - Long Introductions
  - General Talking
  - Break Times
  - Unsuitable samples
  - Discussing Corrective Actions at length

© LAIRDSIDE MARITIME CENTRE

## THE AUDITOR

- ❑ Listener
- ❑ Thorough
- ❑ Objective
- ❑ Fair
- ❑ Accurate Recorder
- ❑ Independent
- ❑ Find Objective Evidence
- ❑ Demonstrate Knowledge
- ❑ Give benefit of the doubt

© LAIRDSIDE MARITIME CENTRE

Questions?

© LAIRDSIDE MARITIME CENTRE

## SUMMARY AND CLOSE Day 4



© LAIRDSIDE MARITIME CENTRE