CANDIDATES

- Please ensure on arrival in class you complete Registration Form provided by Instructors.
- Also provide photographic evidence of identity, i.e. passport, driving licence, discharge book of which a copy will be taken as evidence for Liverpool John Moores University regarding issue of certificates.

WELCOME TO THE

INTERNATIONAL SHIP & PORT FACILITY SECURITY CODE

Ship Security Training Course
June 2014

A Course prepared for

EMSA

DAY ONE

House Keeping

YOUR PRESENTERS

- Phil Davies – Short Course Manager LMC
- John Harris – ISPS & Investigative Trainer

EMSA AGENCY

PRESENTATION

Course Advice

- Mobile Phones off or on Silent during lectures
- This Course is yours! Please ask if you have any requirements.
- Our ultimate aim is that you gain knowledge of the ISPS Code and its application.
- ENJOY THE COURSE!

Course Objectives

Delegates should on completion of the course have an understanding of:-

- Legal Framework and background behind the ISPS Code
- Fundamental requirements of the International Legislation on security (UNCLOS, IMO resolutions and circulars on piracy and stowaways, EU Legislation
- Role of the EU and EMSA
- ISPS Code, its implementation, operation and related background information
- Need and Scope of National Legislation related to the ISPS Code
- Importance of ISPS Code in the supply chain and the concept of intermodel security policy.

Course Objectives Part 2 (S)
Roles and Responsibilities

- The role, tasks and responsibilities of the flag administration
- The role, tasks and responsibilities of a Recognised Security Organizations (RSO) where used
- The link between ISM and ISPS Codes in respect of
  - A Port state control officer (PSCO's)
  - A Duly Authorised Officer (DAO)
  - The role, tasks and responsibility of :
    - Security Personnel
    - Company Security Officer
    - Ships Security Officer
    - Port Security Officer
    - Port Facility Security Officer
    - Staff with Security responsibilities

Course Objectives

- Review of the Operational Issues:

- Ship Security Assessment
- Ship Security Plan
- Declaration of Security
- Verification and certification for ship
- Training requirements
- Drills and Exercises
- Security Levels implementation and control
- Auditing (types of audits) and inspection in relation to ISPS Code
- Control and Compliance measures
- Sanctions

Competencies to be evaluated

During the course it is necessary to evaluate your understanding of the ISPS Code requirements through;

- Participation in open discussions
- Group Exercises and workshops
- Quiz's
- Multiple Choice Self Assessment

Questions ?

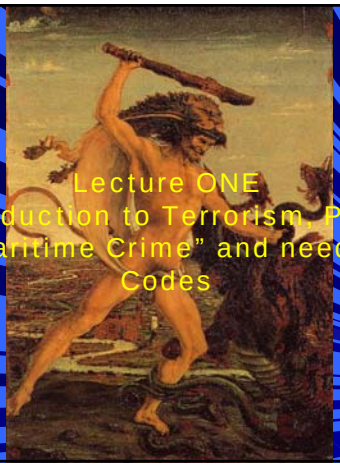
Delegate Introductions

- NAME
- JOB TITLE
- EMPLOYER
- GENERAL EXPERIENCE
- SECURITY EXPERIENCE
- CURRENT KNOWLEDGE OF THE ISPS CODE
- LEVEL OF KNOWLEDGE OF YOUR ADMINISTRATIONS APPLICATION OF ISPS

PRE – COURSE ASSESSMENT

COFFEE

TERRORISM



Lecture ONE
"Introduction to Terrorism, Piracy and Maritime Crime" and need ISPS Codes

WORLD TRADE CENTRE

11 September 2001

Benefits of Maritime Security Measures

- "Maritime security measures were developed in response to perceived terrorist threats. However to varying degrees, the Measures are applicable to countering other forms of security threats, notably piracy and armed robbery in international and territorial waters and unlawful activities such as drug smuggling at Ports. **Thus, the fundamental purpose of the ISPS Code can be considered to be to reduce the vulnerability of the maritime industry to security threats regardless of their nature."**

- Source: Guide to Maritime Security and the ISPS Code 2012

The Terrorist Threat

Abu Sayaaf Group
Somali National Movement
Abu Nidal Organisation
Iran
New Peoples Army
Abyan-Aden Islamic Army/Al-Qai'da
Tamil Tigers
Chechen Dissidents
Israel
Islamic Jihad
Moro Islamic Liberation Front
Algeria
N-17 (Greece)
France
Eritrean Peoples Liberation Front
Popular Front for the Liberation of Palestine
Palestine Liberation Front
15th May Arab Organisation
Jewish Defence League
Knukayin National Union
FARC
Partei Kerkeren Kurdistan
Gerakam Aceh Merdaka

History of Terrorism

- Traced back to earliest recorded History
  - Zealots Jews against Romans
  - **Sicari** Jews off shoot of Zealots against Jews/Romans
- 11th Century
  - "Assassins" – Fanatical Muslims murdered leaders who deviated strict Muslim law.
- 18th Century – Post French revolution
  - Word Terrorism from Robespierre. State terrorism
- Start of modern terrorism mid 19th Century Italian revolutionary - Carlo Pisacane theorised that terrorism could deliver a message to an audience and draw support for a cause - 'Propaganda of the Deed'

Terrorism – Key Features

" The unlawful use or threatened use of Force or Violence by a Person or an Organised Group against People or Property with the intention of intimidating or coercing Societies or Governments, often for ideological or Political Reasons".

A SUMMARY OF THE UK TERRORISM ACT 2000

Modern Terrorism

- 1972: Munich, West Germany: Black September seize Israeli athletes
- 1983: Beirut, US Embassy bombed, later Marine Barracks bombed
- 1993: New York, USA: World Trade Center truck bombed
- 1998: Nairobi and Dar es Salaam Embassies bombed
- 2001: World Trade Centre/Pentagon
- 2002: Bali
- 2004: Madrid
- 2005: London
- 2005: Egypt
- 2005: Bali
- 2005: Jordan
- 2006: Egypt (Dayhl)
- 2006: Israeli warship hit by Hezbollah missile
- 2007: Glasgow Airport
- 2008 : Mumbai Bombings and attacks
- 2009: Attacks in Islamabad
- 2010: Moscow
- 2010: Yemen (Air container bombs)
- 2011: Norway (Internal)
- 2012: Brindisi Italy
- 2012 :Toulouse France Bomb attacks
- 2013: Algeria Gas Plant
- 2013: Boston marathon
- 2014: Multiple incidents Africa/Middle East

Chain of communication between terrorists and citizens

Terrorists → Mass media → Public/Victims

Mechanism of Fear

SANITISATION

London 2005

Victims

- Direct
  - Death, Injury, Trauma
- Secondary
  - Agencies involved in dealing with aftermath
- Indirect
  - Physical/Psychological effects of indirect involvement via media coverage
  - Commercial/Financial consequences
  - Political Consequences

Bali Bombing 2002

- Over 200 Dead
- Over 100 Seriously Injured
- Local Economy Damaged and has taken to 2014 to recover.

- CAN WE ERADICATE ACTS OF TERRORISM?
- THE ANSWER FROM THE EXPERTS IS 'NO'
- HOWEVER WE CAN MANAGE IT, AND THROUGHOUT THIS COURSE, WITH YOUR INCREASED UNDERSTANDING OF THE ISPS CODE WE CAN SHOW HOW YOU HOW

The Maritime Terrorist Threat

Source: McDonald TRANSEC

The Maritime Terrorist Threat

Source: McDonald TRANSEC

Abu Nidal Organisation (ANO)
Liberation Tigers of Tamil Eelam (LTTE)
Haganah
State Sponsored Israel
15th May Arab Organisation (FMAO)
PFLP
PLF
PLO
Chechen Dissidents
Polisario Front
Abu Sayaaf Group (ASG)
Omani Terrorists
Abyan-Aden Islamic Army (IAA)
UNITA
RENAMO
EKAL
PIRA
Irgun Zvai Le'Umi
State Sponsored Algeria
State Sponsored Iran
Islamic Jihad
Gerakam Aceh Merdaka (GAM)
SNM/SPM
Knukayin National Union (KNU)
Cuban Dissidents
Moro Islamic Liberation Front (MILF)
Eritrean Peoples Liberation Front (EPLF)
Jewish Defence Leagque (JDL)
United Jewish Resistance (UJRM)
Partei Kerkeren Kurdistan PKK
Fuerzas Armadas de Venezuelas (FAVLN)
Fuerzas Armadas de Colombia (FARC)
Epanastatiki Organosi 17 (N17)
State Sponsored France
NIJL
New Peoples Army (NPA)

High Profile Maritime Attacks

•1985: Achille Lauro incident-1 killed

USS "COLE"

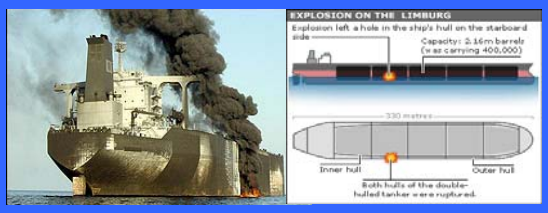
Aden / October 2000 (17 dead - 30 injured)

Use of Ports to conduct attacks

Aden Harbor/Refueling Dolphin

VLCC "LIMBURG"

Off YEMEN 06/10/2002 - Spilled 90,000 bls crude oil



Intelligence –
Only 5 of her tanks were loaded. The strike was specifically aimed at the area of these tanks!
Inside information?

VLCC LIMBURG Update 7/2/2014

The US Defense Department has announced 7/2/14 that the Convening Authority, Office of Military Commissions, referred charges to a military commission in the case of "United States v. **Ahmed Mohammed Ahmed Haza Al Darbi**."

The referred charges allege, among other things, that al Darbi planned, aided and abetted in a course of conduct that resulted in the suicide bombing of the civilian oil tanker **M/V LIMBURG**. Based on these allegations and others outlined in the **charge sheet**, al Darbi is charged with attacking civilians, attacking civilian objects, hazarding a vessel, terrorism, attempted hazarding a vessel, and attempted terrorism.

M. Star - 4/8/2010

Notable Passenger Vessel Incidents

❑ SANTA MARIA	Portuguese	1961
❑ ACHILLE LAURO	Italian	1985
❑ CITY OF POROS	Greece	1988
❑ PRINCESS KASH	Sri Lanka	1998
❑ TRABZON FERRY	Turkey	1996
❑ SUPER FERRY 14	Philippines	2004
❑ SEABOURNE SPIRIT	Somalia	2005
❑ SRI LANKAN PORT –	Sri Lanka	2006

❑ Rare since 2007 but a number of Threats made are causing disruption

Super Ferry 14
27th Feb. 2004

- Voyage - Manila-Cagayam de Oro
- 899 recorded passengers
- TV set taken on board believed to contain a 3.6kg TNT
- Placed on lower decks
- Explosion caused a fire which engulfed the ship.
- 116 fatalities.

Kartepe Ferry-007
Istanbul 11/11/2011

❑ Lone Hi-Jacker
❑ Suicide Vest with
❑ Approx 450g plastic explosive
❑ Turkish Forces boarded 12 hours after the incident and shot dead hi jacker.
❑ Believed to be PKK

The LTTE Terrorist Example

❑ Frequent use of Maritime Target attacks
❑ There were over 40 Suicide attacks from July 1990
❑ Believed to have 3000 Trained marine Personnel in 12 Operational Departments
❑ Has used miniature submarines for conveying suicide bombers inside harbours

- **31/10/2001 Suicide attack on tanker -** A flotilla of five LTTE suicide boats attacked a Point Pedro bound oil tanker carrying over 450 metric tonnes of fuel to the Jaffna peninsula, 12 nautical miles North of Point Pedro yesterday evening.

❑ Have they been defeated????????

PORTS AT THREAT?

Suicide blasts kill 10 Israelis

" A double suicide bombing in the southern Israeli port area of Ashdod has killed at least 10 people.
The blasts went off just before 1700 (1500 GMT) on Sunday in two separate areas of the busy port, witnesses say.

A summit between the Palestinian and Israeli leaders has been postponed indefinitely after the attacks. The al-Aqsa Martyrs' Brigades said it carried out the attack in co-operation with the largest Palestinian militant organisation, Hamas. It is reportedly the first deadly attack on a strategic installation in at least three years of Israeli-Palestinian conflict.

A Palestinian militant had entered the port and asked for water - and the moment he was shown where there was a tap "he blew up" - an employee of the port quoted one of his injured colleagues as saying."

BBC 14/3/04

POTENTIAL MARITIME THREATS

Several groups have a proven capability, notably:

- Al Qa'ida/JI
- LTTE (Sri Lanka)
- Abu Sayyaf
- FARC (Colombia)
- Palestinian factions
- Moro Islamic Liberation Front (MILF)
- Abyan-Aden Islamic Army
  - N-17 (Greece)
  - PIRA (Factions starting to re-appear)

Risk to the individual

March 28, 2013
Bomb Explodes Outside Greek Shipper's Home In Athens

A makeshift bomb exploded outside the home of Nikos Tsakos, the chairman of tanker operator Tsakos Energy Navigation Ltd, police officials said.

A newspaper received a warning call about half an hour before the explosion at the house near the Acropolis

TERRORIST – Ship Owner ?

- OSAMA BIN LADEN (al Qaeda) *before his death* was believed to be a ship owner with a fleet of between 15 to 300 ships, probably flying flags of convenience (FOCs). (Perhaps the most credible estimate of the fleet's size was provided by Norwegian intelligence sources and confirmed by the CIA, both placing the number at 23 vessels.)
- The world is woke up in 2001 to the dangers of allowing shipping to operate under the cloak offered by FOCs:
- Sri Lanka's Tamil Tigers were believed to own a large fleet. There appear to be no accounts of what outcomes the defeat of the LTTE has had on this alleged fleet.
- Has it disappeared? Perhaps not.....

22 Oct 2009

A migrant ship in the early hours in Canadian waters under the name Ocean Lady was identified as the Cambodian-flagged 'Princess Easwary'.

- The ship was owned by Ray Ocean Transport Corp., a company registered in the Seychelles, although its mailing address is in the Philippines, according to shipping records kept by Lloyd's Register.
- The vessel's operator is listed as Sunship Maritime Services, which uses the same mailing address in Cebu, Philippines.
- Alleged LTTE Leaders found on board detained British Colombia officials.

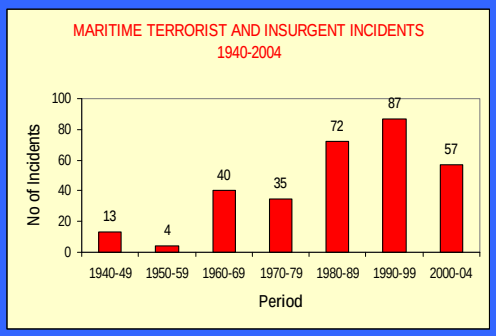
SARA 2003

- The Sara's voyage began on Romania's Black Sea coast
- The Sara was at the heart of an international investigation into the smuggling of terrorists to Europe.
- Flagged to the Pacific island of Tonga –
- One owner wanted by Greek Authorities
- To the Captain's surprise, 14 Pakistani "sailors" came aboard - on the instructions of the ship's owner. All had official seamen's documents and passports which were fraudulently obtained
- False ID & $30000 US found
- Details of Italian Cities and Vatican seized

REALITY OF FOC's

- NATO has investigated a number of vessels which were thought to have terrorist links.
- All fly so-called flags of convenience. They allow owners to hide behind a corporate veil.
- The international seafarers' union says half the world' s merchant fleet uses Flags of Convenience.

International Maritime Attacks



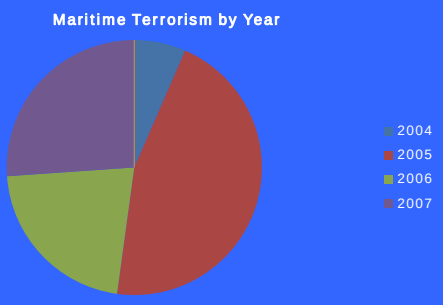
Source – D.McDonald/P.Levey TRANSEC

International Maritime Attacks

Maritime Terrorism by Year														
Year	I	D	W	H		I	D	W	H		I	D	W	H
2004	3	135	0	0	Colombia	12	42	28	38	Bangladesh	2	1	58	0
2005	21	49	70	65	Panama	1	1	0	0	India	2	0	0	0
2006	10	10	8	51	Lat.Am.	13	43	28	38	Nepal	1	0	0	1
2007	12	0	82	56	Iraq	2	3	8	0	Pakistan	1	0	0	18
Total	46	194	160	172	Jordan	1	1	2	0	Sri Lanka	3	0	3	32
Average	12	49	40	43	Lebanon	1	4	1	0	South Asia	9	1	61	51
Maritime Terrorism by Region					M. East	4	8	11	0	France	1	0	0	0
Algeria	1	3	13	0	Indonesia	4	0	12	23	N. Zealand	2	0	2	0
Nigeria	6	1	1	50	Malaysia	1	0	0	3	Others	16	43	30	38
Somalia	1	0	0	0	Philipp.	3	138	32	0	Legend: I: Incidents; D: Deaths;				
Africa	8	4	14	50	Thailand	1	0	0	7	W. Wounded; H: Hostages; M. East:				
					SEA	9	138	44	33	Middle East; SEA: South-east Asia				

Source – Danish Institute for International Studies

2004-2007



Source – Danish Institute for International Studies

MARITIME TERRORIST ATTACKS

- Rare to date - Over last 30 years, Marine targets represent approx 2% of all international terrorist incidents
- Considered difficult to mount - Operating at sea requires more specialised equipment and knowledge
- Publicity aims may not be guaranteed – Unless attacking a high profile vessel or port installation

WHAT IS THE FUTURE?

WHAT IS THE FUTURE?

- Continued search for 'Spectacular' mass casualty targets e.g. 9/11, London, Madrid:
- Arrests in Pakistan/UK and US in Aug 2004 uncovered intelligence illustrating the investment Terrorists are making in planning Spectacular attacks in the UK & US on economic targets.
- The intelligence sought by the Terrorists was more sophisticated and included;
  - Pedestrian flows
  - Potential for collapsing buildings
  - Potential for melting steel infrastructures
  - Details on security check points
  - Movements of employees
  - Changes in Security levels (e.g Sundays)
  - Locations of Emergency services, schools and hospitals

Citigroup Centre

Floors 59
Constructed 1977

WHAT IS THE FUTURE?

- Dhiren Barot is credited with authoring a 39-page memo that advocated the use of simple explosives composed of materials available from local pharmacies and hardware stores. The memo was created for distribution among al-Qaeda operatives and was discovered in 2004 on a laptop in Pakistan.
- On the laptop additional information indicated Al Qa'eda to be considering the value of using a hijacked Tanker as a Terrorist weapon.
- 12/10/06 Dhiren BAROT of N.London convicted Woolwich Crown Court after admitting conspiracy to murder. On 7/11/06 he was sentenced to 40 years.

Source: Secret arrest yielded 'treasure trove'
Daily Telegraph By Peter Foster South Asia Correspondent
(Filed: 03/08/2004)

WHAT IS THE FUTURE?

- The world is now considering measures to address the following types of attack:
- Agro Terrorism – Specifically mentioned in literature seized in Afghanistan
- Bioterrorism – Construction of Biological Weapon

WHAT IS THE FUTURE?

Cyber Terrorism – What could be achieved:

1988 – Robert Morris - Computer Worm

1989 – Legion of Doom – Bell South telephone system.

1997 – Hacker disabled computer system of airport tower - Worcester, Mass.

1998 – NASA, Navy and University computers attacked. Servers were prevented from answering network connections

WHAT IS THE FUTURE?

- Cyber Terrorism – What could be achieved:
- 2001 - MCKINNON hacked into U.S. Military Data Base, and erased information from naval weapons station. UK Home Secretary denies US Extradition request.
- 2007 - Estonia bombarded electronically bringing all communication systems to standstill
- 2010 - Superbug 'STUXNET' computerised 'worm' allegedly bringing Iranian nuclear power processing plant to standstill. Also its alleged availability for sale?
- 2010 - Recognition by most Western Countries now that countering Cyber Terrorist Attack is a priority

WHAT IS THE FUTURE?

- The International participation in Cyber Terrorism
- 2011/2012 - LULZ SECURITY- Group of 7 individuals from US, UK, Holland, Ireland – collectively conspired to embarrass companies agencies and governments re lack of cyber security.
- Hacked into sites including CIA, FBI, SOCA, Sony, Times, Sun, HB Gary, SONY and many more stole and released information or just altered web sites leaving their calling card, i.e. 'LOL'
- 5 of Group subsequently arrested and Charged with Conspiracy. 4 Receiving prison sentences in UK on 6.5.2013 The leader from US Hector MONTSEGUR 29 years awaits trial after assisting FBI in identifying other members .

WHAT IS THE FUTURE?

- In October 2013 Belgian police and Europol released information that 15 people had been arrested after a plot by Drugs Smugglers to import drugs through Antwerp Port in Containers had been smashed.
- The group had hired hackers to infiltrate the computer systems covering container management, to obtain information, passwords, identification numbers and locations of containers in which the drugs where secreted .
- They had then removed the containers prior to the legitimate owners attending the port.
- Subsequent raids by Europol and Belgian police recovered Drugs to vale of £130 million pound, guns ammunition and 1 million pound in cash. (The Daily Telegraph UK 16.10.13)

WHAT IS THE FUTURE?

- What is your Contracting Government doing to assist you in understanding the threat of Cyber Terrorism?
- In UK Contracting Government has issued Guidance and advice to all CSO's and Ports.
- Is this occurring throughout Europe?

MARITIME TERRORISM POTENTIAL

MARITIME TERRORISM POTENTIAL

Tanker movements 18 Feb 2014

Documents reveal al Qaeda's plans for seizing cruise ships, carnage in Europe

- CNN Article By **Nic Robertson, Paul Cruickshank** and **Tim Lister,** CNN May 1, 2012
- May 16 2011, a 22-year-old Austrian named Maqsood Lodin questioned by police in Berlin. He had recently returned from Pakistan via Budapest, Hungary, and then travelled overland to Germany.
- Interrogators found hidden in his underpants were a digital storage device and memory cards.

Maqsood Lodin – Treasure trove of intelligence

- German investigators discovered encoded inside a pornographic video, more than 100 al Qaeda documents that included an inside track on some of the terror group's most audacious plots and a road map for future operations.
- Future plots include the idea of seizing cruise ships and carrying out attacks in Europe similar to the gun attacks by Pakistani militants that paralyzed the Indian city of Mumbai in November 2008.

ATTACK FROM SHORE

CHEMICAL RELEASE

- The global chemical tanker fleet is expanding strongly . Slowed in recent years but expected to increase 1.9% in vessels, (5.6% Deadweight) over next 4 years.
- US imports increased 10% in 2010
- Chemicals are now widely used throughout modern societies and most oil-producing countries have developed refining and petrochemical plants near major centres of oil production.

GAS EXPLOSION

- The carriage of liquefied natural gas (LNG) and liquefied petroleum gas (LPG) by sea has increased dramatically over the last decade or so.
- The international fleet of LNG carriers continues to grow steadily
- New vessels in very large category of between 135,000-140,000 cbm.
- Some analysts think this unlikely
- 5 mile blast zone - SVT

NUCLEAR SHIPMENTS

CONTAINER SHIPMENT

- Estimated 180 Billion TEU's moved Per Annum
- Felixstowe 8000 TEU Per day.
- Only 1- 3% are Checked
- Theft accounts for some;
  - $50Bn US
  - Fraud $150bn US
- Increasing Search by 1% adds 0.5% on value of average TEU

The Low Tech Weapon and Operative Delivery Method !

3873 POTENTIAL HUMAN TARGETS

REVEALED: QE2 TERROR FEARS

Fears that terrorists might seek to crash an aircraft into the QE2 in 1973 were so strong that PM Edward Heath suggested sending the SAS to the ship.

Previously secret papers released last month showed the government feared the Cunard liner would be a "tempting" target for the PLO as it staged a cruise to celebrate the 25th Anniversary of the founding of Israel.

NUMAST Telegraph Feb 2004

WIDER THREATS

- PIRACY
- SABOTAGE
- CRIMINAL ACTS
- MUTINY
- DRUGS TRAFFICKING
- HOSTAGE TAKING
- SURVEILANCE
- COERSION
- SUBVERSION

PIRACY

PIRACY AND CRIME DEFINITIONS PIRACY

The following definition of piracy is contained in article 101 of the 1982 United Nations Convention on the Law of the Sea (UNCLOS):

"Piracy consists of any of the following acts:

(a) any illegal acts of violence or detention, or any act of depredation, committed for private ends by the crew or the passengers of a private ship or a private aircraft, and directed:

(i) on the high seas, against another ship or aircraft, or against persons or property on board such ship or aircraft;

(ii) against a ship, aircraft, persons or property in a place outside the jurisdiction of any State;

(b) any act of voluntary participation in the operation of a ship or of an aircraft with knowledge of facts making it a pirate ship or aircraft;

(c) any act inciting or of intentionally facilitating an act described in sub-paragraph (a) or (b)."

PIRACY AND CRIME DEFINITIONS ARMED ROBBERY

- "Armed robbery against ships" is defined in the Code of Practice for the Investigation of the Crimes of Piracy and Armed Robbery Against Ships (resolution A.922(22), Annex, paragraph 2.2), as follows:

"Armed robbery against ships means any unlawful act of violence or detention or any act of depredation, or threat thereof, other than an act of "piracy", directed against a ship or against persons or property on board such ship, within a State's jurisdiction over such offences."

MSC/Circ.623/Rev.3
29 May 2002

- **PIRACY AND ARMED ROBBERY AGAINST SHIPS**
- **Gave guidance to ship owners, ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships.**
- **It took best practice from around the world.**
- **The Problem did not go away and has now become the major Maritime Security issue**

ATTACKS AND PIRACY

Piracy Jan-June 2014

BOAT or TERRORIST WEAPON ?

"Disabled" by HMS Malborough.
Packed with Explosives – Persian Gulf Feb 2003

Displacement (tons)	2 full load
Length	27.9ft
Beam	7.9 ft
Draft	1.3ft max
Speed	40kts
Propulsion Type	Outboard Gasoline

Seabourn Spirit – Somalia 10/11/05

Attempted attack
100nm from coast

AK-47
RPG-7

Thwarted by on board defences
Long Range Acoustic Device
HP Hoses
Ex-Gurka security staff !!!!

ANTI PIRACY MEASURES

- IMO MSC.1/Circ 1404,1405,1406 Issued 23rd May, 2011.
- Provide guidance in the use Private Contract Armed Security Teams, also
- Provides Governments with guidance in investigating crimes of Piracy and Armed Robbery

- IMO ISSUED UPDATES ON THE ABOVE SUBJECTS IN MSC 1443 19/6/12
- THE HOT TOPIC.

MSC1408
Issued 15/9/2011

- MSC.1/Circ.1408 on Interim recommendations for port and coastal States regarding the use of privately contracted armed security personnel on board ships in the High Risk Area;
- Updated on 16/9/2011 – by MSC1408 Rev2 and subsequently
- MSC 1443 19/6/12 & 1444 25/6/2012

Adopted guidance
at MSC 90 (23 May 2012)

- (Draft) Interim guidance to shipowners, ship operators, and shipmasters on the use of privately contracted armed security personnel on board ships in the high risk area
- (Draft) Interim guidance to shipowners, ship operators, and shipmasters on the use of privately contracted armed security personnel on board ships in the high risk area (revokes MSC.1/Circ.1405/Rev.1)
- (Draft) Interim guidance for flag states on measures to prevent and mitigate Somalia-based piracy

CHAOS OF A DRY-DOCK – Port State Considerations

BLOCKADING PORTS?

HARBOUR OPERATIONS

SEAWARD APPROACHES AND FAIRWAYS

ANCHORAGES

ISPS

- FUNDAMENTAL CHANGE IN SECURITY THINKING.
- WHAT COMES INTO A PORT BY SEA OR LAND, RATHER THAN WHAT GOES OUT ....

Questions ?

Lecture 2

"Maritime Security" (SOLAS V & XI), Intro to EU legislation and ISPS Code

MARITIME VULNERABILITY

- CHOICE TERRORIST TARGET:
  - 90-95% WORLD TRADE MOVES BY SEA AND THE TRADE IS INCREASING
- GENERALLY LAX PORT AND SHIP SECURITY – SHIPS MOST VULNERABLE WHEN AT ANCHOR AND IN PORT
- LACK OF ON BOARD PROTECTION: MUCH REDUCED CREW SIZES
- OTHER BUSINESS OPERATED IN PORT PERIMETERS
- INCREASED INCENTIVES FOR MARITIME CRIME

Trade in Europe

- 80% of EU external trade, 40% intra-Euro trade carried by sea.
- 25% world tonnage is EU member state flagged
- 41% world fleet controlled by EU Companies
- 3.5 billion tonnes of cargo, 400 million passengers pass through EU Port per annum.

POSSIBLE THREATS TO MARITIME INTERESTS

- Al-Qaeda or associated groups may perceive passenger ships as "soft" targets that are relatively easy to attack.
- Operational details may vary according to the attack scenario, but a terrorist operation involving small boats or combat swimmers may feature several common operational elements.
- Operatives would likely conduct research and surveillance of a number of potential targets before selecting one. Operatives then would likely conduct additional surveillance to identify vulnerabilities and to refine their attack plan.
- Operatives involved in the actual assault probably would arrive well beforehand to familiarize themselves with the tactical environment, their equipment, and local security conditions.

B. M. SALERNO
Captain, U.S. Coast Guard
Captain of the Port
Boston, Massachusetts

THE FINANCIAL COST

The following are estimates;-

- USS Cole
  - Implementation $5000 US
  - Repair $240M US
- 9/11
  - Implementation $500K US (but alleged that $250K US retained debt on Credit Cards)
  - Costs $135Bn US – On going $1.7Trn US
- **Bali**
  - **Implementation $30K US**
  - **Cost $120M US + Economic meltdown**
- **Suicide Individual**
  - **$90 – Flexible.**

Source Australian Terrorism Intelligence Centre

ISPS IN CONTEXT

- ISPS came into force 1/7/2004.
- The IMO Stated that there would be NO EXTENSIONS..there were not.

  There have been effects in the US and Europe in respect of denial of access on ISPS Grounds

- However the ISPS Code was in part based upon precedents already in place.....

IMO INITIATIVES

- **NOVEMBER 2001** - IMO SCHEDULES DIPLOMATIC CONFERENCE FOR DECEMBER 2001
- **FEBRUARY 2002** – 1ST ISWG ON MARITIME SECURITY, *PART A*
- **MAY 2002** – MSC 75 FINALISES PART A
- **SEPTEMBER 2002** – 2nd ISWG ON MARITIME SECURITY, *PART B*
- **DECEMBER 2002** DIPLOMATIC CONFERENCE APPROVES SOLAS AMENDMENTS AND ISPS CODE
- **1ST JANUARY 2004** – END OF TACIT ACCEPTANCE PERIOD
- **1ST JULY 2004 – ISPS CODE AND AMENDMENTS WERE ENFORCED INTERNATIONALLY**

SOME MARITIME SECURITY HISTORY

- 1982 UNCLOS - (U.N. Convention of the Law of the Sea)
- 1984 MSC Circ 443 Measures to prevent unlawful acts against Passengers and ships – very much a precursor to ISPS
- Nov 1985 - IMO 14th Assembly adopted Resolution A584(14) - Measures to prevent unlawful acts that threaten the safety of ships and the security of their passengers and crews.
- **Suppression of Unlawful Acts Convention (SUA)** Acts against the Safety of Maritime Navigation **- Adopted 10 March 1988; Entry into force 1 March 1992;**
- Important amendments on the Revision of the SUA Treaties The amendments were adopted in the form of Protocols to the SUA treaties (the 2005 Protocols). **Adopted 14 October 2005; Entry into force 28 July 2010**
- 1996 MSC Circ 754 Security guidance to Passenger Ferries.

WORLD CUSTOMS ORGANISATION

- Established 1952
- 176 Members world wide (Nov 2009)
- Some areas of responsibility are;-
  - UNODC-WCO Container Control Programme
  - Global Supply Chain Security
  - Customs Intelligence
  - Drugs and Chemical Precursors
  - Money Laundering
  - Electronic Crime
  - Firearms
  - Bio terrorism
  - Nuclear and other radioactive materials
- Work Closely with other organisations in anti-terrorism and crime measures

MARITIME POLICY
IMO – ILO Co-operation

- IDENTIFICATION REQUIREMENTS FOR SEAFARERS – CONVENTION PUBLISHED
- UNHINDERED TRAVEL FOR SHIP'S CREWS
- ADEQUACY OF CREW NUMBERS FOR SAFE MANNING OF SHIPS
- MAINTENANCE OF PORT SECURITY
- CONSOLIDATED MARITIME LABOUR CONVENTION –

Seafarers ID Card

- The objective of the Convention is to ensure that Seafarers' identity can be verified positively and authenticated so that they may gain entry to countries without a visa.
- The Seafarers' Identity Document is not intended to be stand-alone travel document. It is to be used in concert with existing travel documents, such as passports or national ID cards, to identify the document holder as a seafarer.

Legality

SUA Convention

- Procedures and actions are provided which can be taken by a State following an attack
- Preventative actions are not prescribe but extends jurisdiction and legal clarity about defences.

SUA Convention
The 2005 Protocol

Added a new Article 3b which states that a person commits an offence within the meaning of the Convention if that person unlawfully and intentionally:

- • when the purpose of the act, by its nature or context, is to intimidate a population, or to compel a Government or an international organization to do or to abstain from any act:
  - uses against or on a ship or discharging from a ship any explosive, radioactive material or BCN (biological, chemical, nuclear) weapon in a manner that causes or is likely to cause death or serious injury or damage;
  - discharges, from a ship, oil, liquefied natural gas, or other hazardous or noxious substance, in such quantity or concentration that causes or is likely to cause death or serious injury or damage;
  - uses a ship in a manner that causes death or serious injury or damage;
  - transports on board a ship any explosive or radioactive material, knowing that it is intended to be used to cause, or in a threat to cause, death or serious injury or damage for the purpose of intimidating a population, or compelling a Government or an international organization to do or to abstain from doing any act;
  - transports on board a ship any BCN weapon, knowing it to be a BCN weapon;
  - transports on board a ship any source material, special fissionable material, or equipment or material especially designed or prepared for the processing, use or production of special fissionable material, knowing that it is intended to be used in a nuclear explosive activity or in any other nuclear activity not under safeguards pursuant to an IAEA comprehensive safeguards agreement; and •
  - transports on board a ship any equipment, materials or software or related technology that significantly contributes to the design, manufacture or delivery of a BCN weapon, with the intention that it will be used for such purpose.

SUA 2005 Protocol

- The new instrument also makes it an offence to unlawfully and intentionally injure or kill any person in connection with the commission of any of the offences in the Convention; to attempt to commit an offence; to participate as an accomplice; to organize or direct others to commit an offence; or to contribute to the commissioning of an offence.
- A new Article requires Parties to take necessary measures to enable a legal entity (this could be a company or organization, for example) to be made liable and to face sanctions, when a person responsible for management of control of that legal entity has, in that capacity, committed an offence under the Convention.
-

EU LEGAL REQUIREMENTS

- Precise legal basis for implementation depend on the adoption of the EU regulation725/2004 (as amended) on enhancing ship and Port facility security and the in a wider context the adoption of EU Directive 65/2005.
- EU regulation does not require transposition into EC Member State Law as it has direct legal effect. However,
- EU Members require their own regulations to give full effect to EU Reg 725:2004. Examples ....
  - UK has applied the international obligation to implement IMO requirements by 1/7/04. SI1495
  - The Republic of Ireland have applied this obligation by introduction SI 413:2004
  - Malta S.L 352.21 Legal Notice 484 of 2004
  - UK is currently reviewing existing and new National Legislation issued to put an enforcement regime in place.

Penalties against whom?

- Most European sanctions apply to Operating Companies and their staff for not fulfilling their obligations in respect of the code.

i.e
- Port operators
- Shipping companies
- CSO, PFSO's SSO's

There is little legislation to assist these individuals in support of their obligations.

Other member states?

- What are the legal sanctions in delegates states?
- Croatia O SIGURROSNOJ ZASTITI POMORSKIH BRODOVA; LUKA (nn 124/03, 53/12) , PROGLAŠENJU ZAKONA O SIGURNOSNOJ ZAŠTITI POMORSKIH BRODOVA I LUKA 3096
- Poland Regulation from 17.06.2004 Dzrennik Ustow Nr. 172 from 4.08.2004 Poz 1801
- Romania – 484 Nov 2003
- Sweden - 437 2004
- Slovenia – Governmental Decree 2904 12/06/2004 OJ RS 64/2004 Ammended 41/2007

ISPS CODE & LEGAL ASPECTS

- IMO requirements are comprehensive but....
- They DO NOT set out specific Security Standards so as an example.....
  - The UK considers such standards are necessary in the UK to ensure effective security which is consistent across all Ships and UK Port Facilities.
  - The Ship and Port Facility Security Regulations 2004 (SI1495) provides a mechanism by which the SoS for Transport will issue legally binding Directions to Harbour authorities and operators and UK Shipping Companies.

ISPS Preamble

- Paragraph 5.
- "...it was also agreed that the provisions *(of the ISPS Code)* should not extend to the actual response to attacks or to any necessary clear up activities after such and attack."

ISPS CODE

Applies to the following types of ships engaged on international voyages :-

- Passenger ships including high speed vessels
- Cargo ships including high speed vessels of 500 gross tonnes and upwards
- Mobile off-shore drilling units (MODU)
- Port facilities serving such ships engaged on international voyages

WHAT IS A PORT FACILITY

SOLAS XI Reg 2 - DEFINITIONS

- A port facility is defined by the IMO as a location, as determined by the Contracting Government, where interactions occur when a ship is directly and immediately affected by actions involving the movement of persons, goods or the provision of port services to or from the ship.
- It includes areas such as anchorages, waiting berths and approaches from seaward.
- The IMO's definition of a port facility in practical terms, can therefore be an individual berth, wharf or terminal.

WHAT IS A Ship/Port Interface

SOLAS XI Reg 1.8 - DEFINITIONS

- A Ship to Port Interface means the interactions that occur when a Ship is directly and immediately affected by actions involving the movement of persons, goods or the provision of Port Services to or from the Ship

What is a Security Incident?

SOLAS XI Reg 1.13 - DEFINITIONS

- *Security incident* means any suspicious act or circumstance threatening the security of a ship, including a mobile offshore drilling unit and a high speed craft, or of a port facility or of any ship/port interface or any ship to ship activity.

WHAT IS A Ship/Ship Activity

SOLAS XI Reg 1.10 - DEFINITIONS

- A Ship to Ship Activity means any activity not related to a port facility that involves the transfer of goods or persons from one Ship to another.

WHAT IS A Designated Authority

SOLAS XI Reg 1.11 - DEFINITIONS

- Designated Authority means the organization(s) or administration(s) identified within the Contracting Government as responsible for ensuring the implementation of the provisions of this chapter pertaining to port facility security and ship/port interface, from the point of view of the port facility.

THE 3 LEVELS OF SECURITY

SECURITY LEVEL 1

Normal – The level which ships and port facilities normally operate.

SECURITY LEVEL 2

Heightened – The level applying for as long as there is a heightened risk of a security incident.

SECURITY LEVEL 3

Exceptional – The level applying for the period of time when there is a probable or imminent risk of a security incident.

ISPS CODE – 19 ELEMENTS

Internationally
PART A- MANDATORY
PART B – GUIDANCE

BUT!!!!!!! for Europe
EU Regulation No 725/2004 makes many sections of Part B mandatory especially Drills & Exercises.

ISPS
CONTRACTING GOVERNMENT INSPECTIONS

- The contracting government will determine the security level for Port facilities and Ships in their territory and under their Administration.
- Conduct Port Facility Security Assessments.
- Will verify the validity of the international ship security certificate.
- Will control or deny access to the port or movement within the port.

SHIP ISPS COMPLIANCE

Install Equipment (AIS, SSAS etc)
Issuance of a Continuous Synopsis Record (CSR)
Carry out Ship Security Assessment (SSA)
Appoint Company & Ship Security Officers (CSO & SSO)
Develop and submit Ship Security Plan (SSP)
Implement Security training, drills, auditing
Inspection by Flag (Approved RSO)
Maintain Records
Administration of Declarations of Security
International Ship Security Cert Issued
Maintain the Plan

PORT FACILITY ISPS COMPLIANCE

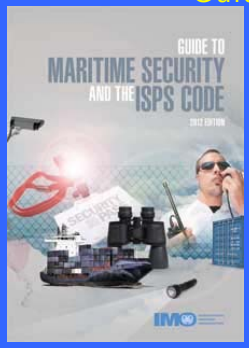
Port Facility Security Assessment undertaken
Appoint Port Facility Security Officer (PFSO)
Possibly undertake Counter Terrorist Checks
Develop Port Facility Security Plan
Undertake PFSO and Facility Staff Training
Port Facility Security Plan Approved & Implemented by Contracting Government
Implement Security training, drills, auditing
Maintain the Plan

SOME ABREVIATIONS

PFSO –	Port Facility Security Officer
SSO –	Ship Security Officer
CSO –	Company Security Officer
PFSA –	Port Facility Security Assessment
PFSP –	Port Facility Security Plan
SSA –	Ship Security Assessment
SSP –	Ship Security Plan
RSO –	Recognized Security Organisation
DOS –	Declaration of Security

(SEE COURSE NOTES FOR A FULL LIST AND DEFINITIONS)

Guidance



IMO Publication, 2012.
Perhaps 8 years too late!

Questions?

Exercise 1

'THIS IS THE FUTURE'

This is the Future – The situation

COFFEE

Lecture THREE
"Risk Assessment"

CODE OF PRACTICE ON SECURITY IN PORTS

IMO/ILO
MESSHP/2003/14
Appendix A - PSA

Although aimed at Ports, it provides a very satisfactory methodology for risk assessment on ships.
IMO Guide 2012 provides guidance and a methodology.
TRAM is a simplified version of this
In addition the US NVIC 10-02 provides an alternative methodology – used by some RSO's undertaking the SSA.

Maritime Security Threat

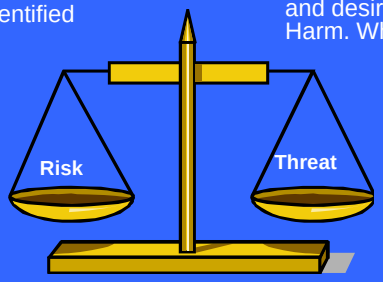
IMO/ILO Code of Practice on Security in Ports

- THREAT – The likelihood that an unlawful act will be committed against a particular target, based on a perpetrators intent and capability.
- As long as intentions and capabilities exist, Security threats EXIST .
- Addressing one of the elements will reduce the risk of threats.

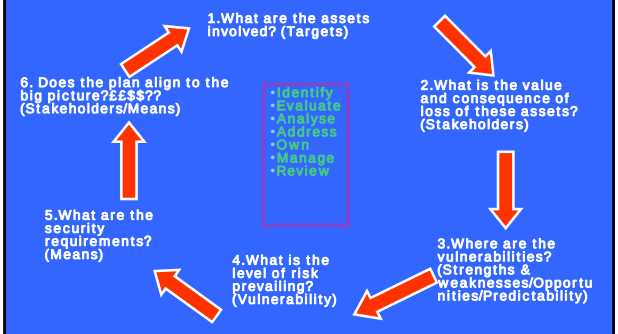
The Balance of Risk and Threat

Exposure to the identified threat

The capability and desire to Harm. Who?



Managing Risks



RISK ASSESSMENT METHODOLOGY

- THREAT and
- RISK
- ASSESSMENT
- MATRIX
  - Identify Threats
  - Initiate and recommend countermeasures
  - To Deter, Detect, Reduce consequences
  - To enable planning and Resource allocation

THREAT SCENARIOS 1

Consider Threat scenarios.
Ships and the Port Facilities they interface with which are vulnerable.

Direct Attack
- Injury/Loss of Life

Destruction of Facilities and Infrastructure
- Hi-Jack of vessels
- Use as a weapon

Release of Noxious or Hazardous material.
- Use as a weapon

Sabotage

Kidnap and Ransom

THREAT SCENARIOS 2

AREAS OF RISK MAY INCLUDE;-

VESSELS
- Command areas (Bridge , E.R)
- Machinery Spaces
- Cargo Spaces
- I.T and Communications infrastructure
- Areas of special vulnerability (e.g Cargo Discharge points)

THREATS IN THE PORT ENVIRONMENT
- Cargo Gear
- Lock gates
- Radar Towers
- Impounding Stations
- Tank farms
- Rail Links
- Access Points
- Piers/Quayside and Vessels alongside

Personal security !!

THE THREAT 1

- Probability of an incident to be assessed using the following scale;

  3 - HIGH
  2 - MEDIUM
  1 – LOW

- Threat Score based on Specific information or Known Characteristics of Potential Target

VULNERABILITY 1

TO BE ASSESSED AS FOLLOWS

- 4 = No existing security measures or ineffective security measures.
  - Unrestricted access.
  - No monitoring
  - Untrained Staff
- 3 = Minimal Security measures.
  - Inadequate Access Control
  - Sporadic Monitoring
  - Poor Training

VULNERABILITY 2

TO BE ASSESSED AS FOLLOWS

- 2 = Satisfactory Security measures
  - Controls on access.
  - Formal Security Training programme
  - Target not easily damaged
- 1 = Fully effective Security measures.
  - ALL OF "2" PLUS.....
  - Ability to move to Higher Levels of Security
  - Target difficult to damage
  - Capable of operating if some functions damaged

THE RISK – Value/Consequence

What is consequence of loss ?

Loss of life – litigation, insurance, reputation, emotional consequences
Loss of ship – expense, reputation, business expectancy
Loss of cargo – expense, reputation, business expectancies

Loss of reputation – market credibility, shareholder confidence, jobs.

IMPACT (Consequence) 1

Assess Impact on each potential target;

- 5 = Detrimental to Security and Safety
  - Loss of Life or serious injury
  - Widespread danger to Public Health and safety

Note. Loss of life needs to be considered in the widest context. e.g Framework for conducting Security Assessments.
4 – Substantial – Multiple fatalities (5)
3 – Significant – Loss of life (4.75)
2 – Moderate – Major injuries (4.5)
1 – Minor – Minor injuries (4.25)

- 4= Detrimental to Public Safety/National Prestige
  - Significant Environmental damage
  - Localised Public Health and safety compromised

IMPACT (Consequence) 2

Assess Impact on each potential target;

- 3 = Detrimental to Environment/Economic functioning of the Port Facility and vessel operations
  - Likely to cause sustained Port wide disruption
  - Significant economic loss
  - Damage to National Prestige
- 2= Detrimental to Assets, infrastructure, utilities and Cargo Security
  - Limited disruption to individual assets/organisation
- 1 = Detrimental to Customer and/or Port community confidence

RISK SCORE

Risk Score is;-

- THREAT x VULNERABILITY X IMPACT
- HIGHEST SCORE SCENARIO WILL BE;-

THREAT HIGH	3
VULNERABILITY – NO COUNTERMEASURES	x4
IMPACT – LOSS OF LIFE/INJURY	x5
	60

LOWEST SCORE SCENARIO = 1 x 1 x 1 = 1

ACTION PRIORITY 2

- Tabulating and Listing Scores for Each Threat Scenario will assist in setting priorities for Dealing with potential incidents

AND

- Provide indication of actions needed to
- DETER
- DETECT and
- MITIGATE CONSEQUENCES
- DEPLOY APPROPRIATE RESOURCES AND SECURITY MEASURES

ACTION PRIORITY 1

- Decide on a priority basis what your actions should be protecting your facilities from incidents and attack.

- Select an option against your Risk Score.
  - **1 Do nothing**
  - (Low score 1 to 5)
  - **2 Check current security measures** (TOLERABLE)
  - (Low to Middle score 5 to 15)
  - **3 Improve existing security measures** (MANAGEABLE)
  - (Middle score 15 – 40)
  - **4 Improve and increase all security measures** (UNACCEPTABLE)
  - (High score 40 – 60)

THE RISK

Manage the risk
Implement plans
Own the risk
Take responsibility for solutions

THE THREAT

Threat assessment information sources:-

- Contracting government
- Foreign Governments
- EMSA
- Security services
- Risk Management Services
- Web sources
- Police – Special Forces Sections
- PFSO's
- CSO's

Lecture FOUR
"ISPS Code in Detail"
PART A

ISPS PART A, SOLAS CHAPTER V & XI

- DOCUMENT REVIEW & RECAP

SUMMARY AND CLOSE DAY 1

DAY 2

June 2014 revision

A Course prepared for

EMSA

QUESTIONS FROM DAY 1?

VIDEO 1
'Security, Everybody's business'
A Training guide

Lecture FIVE
"ISPS Code in Detail"
PART B

ISPS CODE PART 'B' - QUIZ

PART B Debrief & Issues

MSC/Circ.1097

International Ship Security Certificates (ISSC)

8 The Committee recognized that part B of the ISPS Code was albeit recommendatory, a process all parties concerned needed to go through in order to comply with part A. It was concluded that paragraph 9.4 of part A of the ISPS Code required that in order for an ISSC to be issued, the guidance in part B would need to be taken into account.

9 The Committee further specifically considered that an ISSC would not be issued unless paragraphs 8.1 to 13.8 of part B of the ISPS Code had been taken into account.

Mandatory provisions

EU REGULATION 725:2004

Makes;
— 1.12 (revision of ship security plans),
— 1.16 (port facility security assessment),
— 4.1 (protection of the confidentiality of security plans and assessments),
— 4.4 (recognised security organisations),
— 4.5 (minimum competencies of recognised security organisations),
— 4.8 (setting the security level),
— 4.14, 4.15, 4.16 (contact points and information on port facility security plans),
— 4.18 (identification documents),
— 4.24 (ships' application of the security measures recommended by the State in whose territorial waters they are sailing),
— 4.28 (manning level),
— 4.41 (communication of information when entry into port is denied or the ship is expelled from port),
— 4.45 (ships from a State which is not party to the Convention),

EU REGULATION 725:2004

— 6.1 (company's obligation to provide the master with information on the ship's operators),
— 8.3 to 8.10 (minimum standards for the ship security assessment),
— 9.2 (minimum standards for the ship security plan),
— 9.4 (independence of recognised security organisations),
— 13.6 and 13.7 (frequency of security drills and exercises for ships' crews and for company and ship security officers),
— 15.3 to 15.4 (minimum standards for the port facility security assessment),
— 16.3 and 16.8 (minimum standards for the port facility security plan),
— 18.5 and 18.6 (frequency of security drills and exercises in port facilities and for port facility security officers).

COFFEE

Lecture SIX
"Ship Security Assessment"

What is a Ship Security Assessment (SSA)?

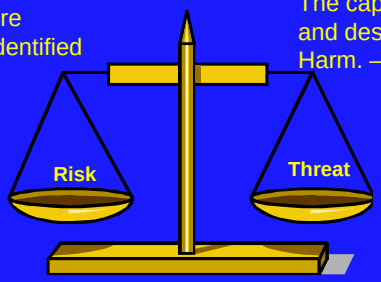
The SSA is a process by which competent persons identify key assets on board a ship and assesses the threats to these assets and identifies security measures that can be implemented to reduce the vulnerability of these assets.

WAS & IS FIRST STAGE OF COMPLYING WITH ISPS REQUIREMENTS

The Balance of Risk and Threat

Exposure to the identified Threat

The capability and desire to Harm. – Who?



Framework for conducting security assessments.

- Section 4 – Security responsibilities of ship operators and
  - 4.7 SSA guidance
- Section 5 Risk assessment methodology

Who will undertake the SSA?

8.1 The Company Security Officer (CSO) is responsible for ensuring that a Ship Security Assessment (SSA) is carried out for each of the ships in the Company.s fleet which is required to comply with the provisions of chapter XI-2 and part A of this Code for which the CSO is responsible.

While the CSO need not necessarily personally undertake all the duties associated with the post, the ultimate responsibility for ensuring that they are properly performed remains with the individual CSO.

SHIP SECURITY ASSESSMENT No. 1

- Assessment will be carried out by Competent persons
  - It will be ship specific.
  - It will be risk based.
  - It will be based on specific threat scenarios
  - It will involve an on site survey.
  - It will form the basis of the SSP.
  - The SSA must be protected from unauthorised access or disclosure.
- Upon completion of the SSA, a Report shall be prepared which forms the basis to develop the plan.

Responsibility of Contracting Governments

- Administrations are responsible (SOLAS XI_2 Reg. 3) for providing guidance to CSO's on the security risks that their ships may face on voyages, having regard to,
  - the ship type,
  - the sea areas in which the ship operates and
  - the ports and port facilities that it uses.
- If a ship changes its trading pattern, the security threats that it faces may significantly change;
- In such cases Administrations should be well placed to provide guidance on any new threats that the ship may face as a basis for updating the SSA

SOURCE - Guide to Maritime Security and the ISPS Code

SHIP SECURITY ASSESSMENT No. 2

Sect 8 Part A

8.4 The ship security assessment shall include an on-scene security survey and, at least, the following elements:

.1 identification of existing security measures, procedures and operations;

.2 identification and evaluation of key ship board operations that it is important to protect;

.3 identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritise security measures; and

.4 identification of weaknesses, including human factors in the infrastructure, policies and procedures.

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

SHIP SECURITY ASSESSMENT No. 3

PART B – 8.8

- The SSA should consider the persons, activities, services and operations that it is important to protect. This includes:
  - .1 the ship's personnel;
  - .2 passengers, visitors, vendors, repair technicians, port facility personnel, etc;
  - .3 the capacity to maintain safe navigation and emergency response;
  - .4 the cargo, particularly dangerous goods or hazardous substances;
  - .5 the ship's stores;
  - .6 the ship security communication equipment and systems, if any; and
  - .7 the ship's security surveillance equipment and systems, if any.

SHIP SECURITY ASSESSMENT No. 4

Part B - Sect 8.9

- The SSA should consider all possible threats, which may include the following types of security incidents:
  - .1 damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism;
  - .2 hijacking or seizure of the ship or of persons on board;
  - .3 tampering with cargo, essential ship equipment or systems or ship's stores;
  - .4 unauthorized access or use, including presence of stowaways;
  - .5 smuggling weapons or equipment, including weapons of mass destruction;
  - .6 use of the ship to carry those intending to cause a security incident and/or their equipment;
  - .7 use of the ship itself as a weapon or as a means to cause damage or destruction;
  - .8 attacks from seaward whilst at berth or at anchor; and
  - .9 attacks whilst at sea.

PART B 8.7

As Mandatory - Article 3 of EC 725:2004

The SSA should consider the continuing relevance of the existing security measures and guidance, procedures and operations under both routine and emergency conditions and should determine security guidance

Ship & Port Restricted Areas

Part A 7.2.4 & 14.2.4 : Monitoring restricted areas

…to ensure that only authorised persons have access

Ship Access - Environment/perimeter/access?
Internal security:, surveillance; identity checks, searching, extra vigilance, port vehicle controls?

Emergency Response

- This will require review of the response likely at the Port Facilities where the ship trades.

Environment

Environment

Secure anchorage? : What is the Threat from terrorists, pirates, stowaways.

Are there Water Patrols, aerial surveillance, over side illumination, ?

Frequency and effectiveness of patrols
Supervision of those on board and around the ship?

ACCESS CONTROL

ID system, visitor control, RA Designation, The Port interface.

Security doors, barriers, lighting Surveillance equipment,

Part B 8.7.5 and B15.16.1: controlling Access

Part B 8.4.13; Ship & Port Operations

Port rules for entry? Scheduled? Aware of security level?

Crew ID? Security procedures on arrival? SSO/PFSO's briefed? Who else is in port?

COMMUNICATIONS

A7.2.7: Security communications must be readily available

- Back-Up Systems
- Continuous and robust communication methods
- Secure/Private
- Integrated?
- B8.3.5 radio and telecommunications systems, including computer systems and networks;

I.T. – SECURITY MANAGEMENT

- Clear policies on use of IT
- IT Security awareness training
- Monitoring of buyers or auditors of software
- Password rules applied and enforced
- Clear Logging on and off regulations
- Authentication of callers requesting information
- Personnel Department input, past employee control and disgruntled staff
- Procedures and checks to ensure compliance with the any legislation e.g Data Protection Act 1998 in UK

CARGO HANDLING

A7.2.6 and (A14.2.5): supervising the handling of cargo

SHIPS STORES

Part A 7.2.6: (A14.2.6)supervising th handling of ship's stores
Source?
Integrity?
Reconciliation?
Their Storage?

SSA Considerations

- WHY WOULD THE VESSEL BE A TARGET ?
- SECURITY STRENGTHS
- SECURITY WEAKNESSES
- SECURITY OPPORTUNITIES
- PREDICTABILITY OF AN INCIDENT ?
- VULNERABILITIES BOTH PHYSICAL AND HUMAN
- STAKEHOLDERS
- MEANS OF MITIGATION

SHIP SECURITY ASSESSMENT 6

- ON COMPLETION OF THE SSA;-
- IT FORMS THE BASIS OF THE SHIP SECURITY PLAN
- IT MUST ACCOMPANY THE SSP
- APPROVAL OF THE ASSESSMENT IS NOT REQUIRED
- IT NEED NOT REQUIRED TO BE RETAINED ON BOARD

Questions?

LUNCH

SSA Exercise 2

EXERCISE 2

PRACTICAL SHIP SECURITY ASSESSMENT

COFFEE

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?

EXERCISE 3
ACCESS - SUCCESS

Lecture EIGHT
"ISPS AND ISM"

Safety versus Security

- Sometimes there are conflicts between SAFETY and SECURITY
- We saw the dilemma for the ships Master.
- Refer to SOLAS XI-2 Regulation 8.

ISM – A Phased initial approach

- Guidelines on implementation adopted by IMO Resolution A.788(19) 23rd Nov 1995
- Became mandatory under the SOLAS Ch IX provisions 1st July 1998 for Passenger ships and HSC, tankers (oil, chemical, gas), bulk carriers and cargo HSC's of 500gt and above.
- Extended to all cargo vessels of 500gt and above from 1st July 2002
- ISPS a one phased approach – little time for integration and harmonisation.

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

Regulation EC No.336/2006

- Repealed EC No 3051/95
- Extends ISM requirements to domestic operations and between member states
- There are 'opt out' provisions.

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.

- Identify WHO has Responsibility for the ship
- Document and define the responsibility and interrelationships of those affecting safety and pollution prevention.
- Provide adequate resources and shore based support to DPA

ISM 4 & 5

- Designated Person – Direct access to highest management level.
- 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?

SUMMARY AND CLOSE

Day 3
Questions related to DAY TWO?

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 Maritime 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?

UK Example

- 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 - LATVIA require that a Security Plan review should be taken at least every 6 months and
  - UK - MUST be reviewed when;
    - The relevance of the Security Assessment has been affected by Operational Changes.
- OTHERS?

Questions?

Lecture TWELVE
"Security Equipment"
13.1.5 13.1.16 Part B

SECURITY EQUIPMENT

Examples of Security Equipment and Systems

- GMDSS
- SSAS
- AIS
- LRIT
- RADAR
- Ships Defences -Razor/Barbed Wire anti climb fencing, Water Foam Monitors
- Security Glass
- Signs
- Barriers
- Access Control

- Locks
- Seals
- Lighting
- Crew PPE
- Communication systems (Radios)
- Closed circuit TV
- Metal detectors (AMD, HHMD)
- Baggage X-ray equipment
- LRAD, MAD

SHIP SECURITY ALERT SYSTEM

- Ships were required to fit a Ship Alert System not later than 1st July 2006.
- Covert Alarm Systems will alert the Company/Competent Authority.
- If a Ship Alert is initiated and verified, via Company/Government who will take the necessary action.

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

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

OVERT ALERTING – e.g PIRACY ATTACK

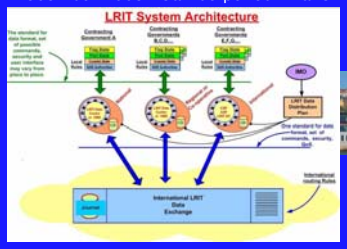
AIS

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

Initially a Safety Measure, but can be used for Maritime Security and has been viewed by many states in this context.

Long Range Identification & Tracking

Long Range Identification & Tracking
LRIT – Introduced from 1 January 2008 and applies to ships constructed on or after 31 December 2008 with a phased-in implementation schedule for ships constructed before 31 December 2008. Can be polled. Transmission every 6 hours.



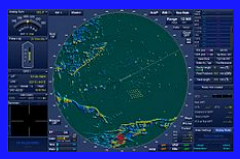
EMSA – European LRIT Data Centre

GENERAL 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.

RADAR

RADAR – RADio Detection And Ranging.
Use of electro magnetic waves for the detection of Targets. Radio navigation device can be used for Security long range scanning.



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.

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.1406/Rev.2
(Revokes MSC 1/Circ. 1406/Rev1}
Flag State interim guidance on use of PCASP

MSC.1/Circ.1405/Rev.2
Revised Interim guidance to ship owners, ship operators and shipmaster on
the use of PCASP on board ships in the High Risk Area (revokes MSC. 1/Circ.1405/Rev.1)

ISO/PAS 28007/2012
Applicable to PCASP

KEVLAR (ANTI BALLISTIC)JACKETS

Provides protection to crew in respect of armed pirates.

CITADEL

A FORTRESS TO PROTECT THE SHIP.

SHIP DEFENCES – ELECTRICAL FENCING, RAZOR WIRE, ANTI CLIMB FENCING

Mesh Fencing

Razor Wire

Anti climb 'Rat Trap

Electric Fencing

BULLET PROOF GLASS

Bullet proof/non shattering glass is now being used more and more within the Maritime environment.

The cost however is prohibitive, therefore private yachts are more likely to have it fitted.

Although it is available for commercial shipping especially for vessels using high risk routes.

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.

SHIPBOARD LIGHTING

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

SIGNS

- Can give a strong signal about security awareness in on a Ship and Port
- Can be a form of deterrent against unauthorised access
- Must be used to denote Restricted Areas i.e. Bridge, Engine Room
- Specific wording to comply with EC requirements (See notes)
- Must be used to advise where CCTV is used

BARRIERS – WHAT BARRIERS ?

SHIPS ENVIRONMENT & SAFE EGRESS

KEY PAD ACCESS

QUALITY LOCKS

BS 3621-1980.

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

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.

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

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

SCREENING EQUIPMENT

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

- These systems must be augmented by a physical search of a set proportion of those being screened.

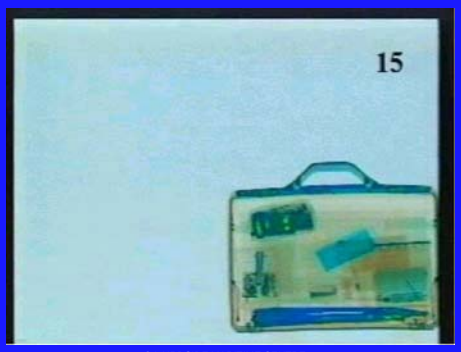
- B 9.38/B16.45
  - Double screening not envisaged. If Port equipped then responsibility to screen lies with the Port.

METAL DETECTORS

AMD – HHMD
Environment &
Calibration
Limitations

X-RAY SCANNERS

X-RAY INTERPRETATION

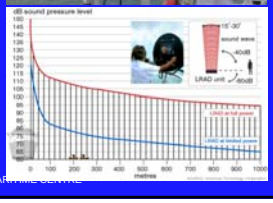


MAGNETIC AUDIO DEVICES

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

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



BOMB SUPRESSION

- BOMB BLANKETS
- BLAST SUPRESSION BINS

1 kg TNT Uninhibited & Inhibited

RUNNING GEAR ENTANGLEMENT

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

ACCESS CONTROL- PASS SYSTEMS

- THE CODE ADVISES THAT A PASS SYSTEM SHOULD BE IN PLACE BUT IT IS NOT MANDATORY.
- CAN BE USED FOR SHIPS OR PORT FACILITIES TO CONTROL ACCESS TO:-
  - SHIPS
  - RESTRICTED AREAS (R.A.)
  - PORT FACILITIES
- AIDS IDENTIFICATION
- PASS SYSTEMS ARE EFFECTIVE WHEN CO-ORDINATED

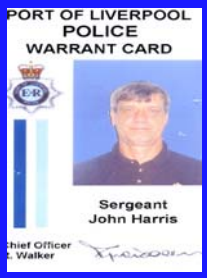
SEAFARERS ID CARD

•The objective of the Convention is to ensure that Seafarers' identity can be verified positively and authenticated so that they may gain entry to countries without a visa.

•The Seafarers' Identity Document is not intended to be stand-alone travel document. It is to be used in concert with existing travel documents such as passports or national ID cards, to identify the document holder as a

ACCESS CONTROL- PASS SYSTEMS

TRANSEC INSPECTORS



POLICE WARRANT CARD

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)

Questions ?

Questions?

LUNCH

IMO Guidance

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

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

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?

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);

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

Identify threats... establish proportionate security measures

Who wants to?... Why us?... How can they?

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

Reporting Form

- See Page 39-40 of Notes.
- SHIP PRE-ARRIVAL SECURITY INFORMATION FORM
- New Format ??

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.

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.

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

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.

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.

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

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.

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.

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).

Also see Guide to Maritime Security and the ISPS Code 2012 Edition Sect 2.7.17

MSC/Circ.1132
14 December 2004

Para 13

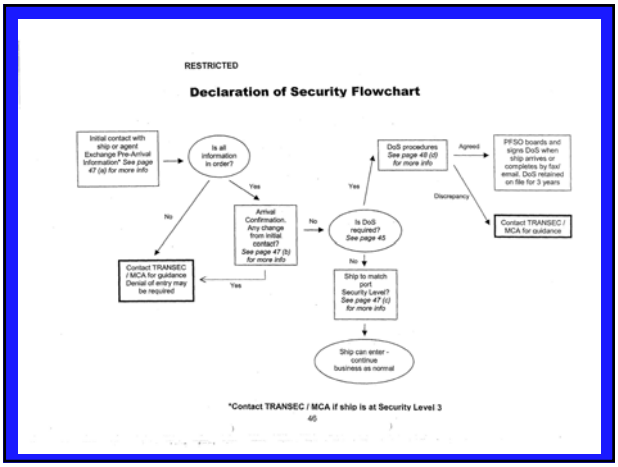
The DoS is intended to be used in exceptional cases usually related to higher risk, when there is a need to reach an agreement between the port facility and the ship as to the security measures to be applied during the ship/port interface because, either the provisions of the PFSP and of the SSP did 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.

Maritime Security and the ISPS Code 2012 Edition

- 2.7.4
- The requirements to request a DOS, and those relating to the response to such requests, should be based on security considerations. Declarations of Security should never be the norm and should not normally be required when both the port facility and ship are operating at Security Level 1.
- Section 2.7.5 provides a useful matrix.

DoS ADMINISTRATION

- Ensure that the form of DoS accords with the Model in Appendix 1 Part B 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/Portugal /Netherlands Minimum of **3 years** for both ports and ships. Spain 5 years.
- Lower 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.



Ship & Port Environment

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

How do other member states control Access?

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.

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.

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.

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

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

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

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

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*

PROTECTION & PREVENTION
Basic

Deter – detect – react!

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

AREAS FOR CONCEALMENT

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

Common sense measures

BOARDER REPELLING METHODS

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.

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

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.

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

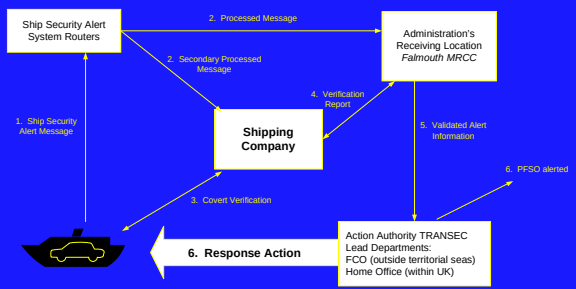
.3 a system may utilise the exchange of messages containing key words between a ship and, typically, the Company.

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

SHIP SECURITY ALERT IN PORT

- Ships are required to fit a Ship Alert System not later than 1st 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

SHIP SECURITY ALERT SYSTEM



Source:

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**

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

The Response?

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,

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"**

Questions?

COFFEE

EXERCISE 4
OPERATION 'DIGITAL'

Questions?

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.

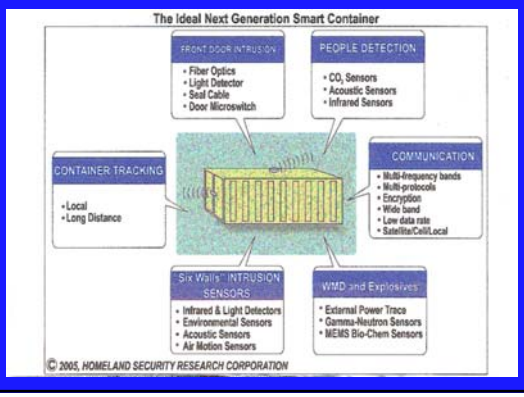
CONTAINER SECURITY INITATIVE

- 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)
- 58 Ports worldwide up to November 2013 - (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 now allows mutual recognition agreement with US ~Customs
- 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.

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 53 countries having introduced/ and 10 are 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.

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

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.

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. i.e. 53 other countries
  - ISO 28001 - 28003 provides accreditation for implementation of Security Management systems, Best Practice for Implementing Supply Chain Management, Auditing systems for Supply Chain Management.

AUTHORISED ECONOMIC OPERATOR - INCENTIVES

- In November 2013 a revised European Union Customs Code was introduced, which has to be implemented in full by the 1.5.2016.
- The code introduces the requirement for a 'Guarantee' to be in place for all Customs Duties approved due through the operation of Customs Authorised Relief or suspension schemes which many companies use. Estimated in UK 20,000 annually
- Banks may provide such a 'Guarantee', but they may want up front costs or may not want to involve themselves in such, or may even require or impose security risk assessments on companies before assuring such 'Guarantees'.
- This will substantially increase costs to companies in any customs authorisations they seek.
- HOWEVER AEO ACCREDITATION WILL ENSURE SUCH 'GUARANTEES' ARE WAIVED BY CUSTOMS.

QUESTIONS?

LECTURE 14
TRAINING REQUIRMENTS

SECURITY TRAINING SHIPS - ISPS Code 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.

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

MSC/Circ.1154
T2/4.2 23 May 2005

- **GUIDELINES ON TRAINING AND CERTIFICATION FOR COMPANY SECURITY OFFICERS**

MSC/Circ.1235
21st 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.

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

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.

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

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
  - DfT (TRANSEC) – Port Facility Security Officers
- Training Providers approved and courses verified and audited

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)

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 COMPETANCIES 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 SPECIFICATION

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.

EUROPEAN METHODS

?

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?

Regulation STCW AI/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-I/6 of the STCW Code for the type and level or training or assessment involved.

STCW AI/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

Qualification requirements for trainers and assessors

- Should be meeting the requirements of STCW BI/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

IMO Model Course 6.09

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

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 ships 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 and would have as a minimum a Cert of Proficiency in Security Duties.

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 if provided
- Staff should be able recognise weapons and devices
- Refresher training should ideally be undertaken on a regular basis

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.

IMO Guide 2012

Training requirements Government Officials

- Appropriate knowledge levels specified
- Advises a National curriculum
- 12 points are considered as a minimum

- Experience to date shows;
  - Courses should be 6-12 participants
  - Workshops supplement training on 'Administrative and Communication skills'
  - Requires on going and specialised training
  - Should participate in exercises

DAO Training.xps

CODE OF GOOD PRACTICE FOR PORT STATE CONTROL OFFICERS

- MSC-MEPC.4/Circ.2 1 November 2007

INSTRUCTIONAL TECHNIQUES 1

Information can be passed on by;

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

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

TRAINING VALUE ?

Questions?

Lecture 17
AUDIT
and REVIEW/VERIFICATION

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

Auditing

TWO LEVELS

1. Internal – Shipping Company requirements
2. External – 2nd and 3rd Party

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.

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

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

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.'

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.

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.

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

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

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

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;

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.

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 !!!!

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

REVIEW

- REVIEW - To examine again.

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.

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.

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

AUDITING PROCESS 2

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

Preparation for the Audit

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

Checklists

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

Opening the Audit

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

Audit

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

Closing the Audit

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

Documented System

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

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

Conformance or non conformance???

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

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

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

Audit Types

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

Audit Tools - QUESTIONS

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

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

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

THE AUDITOR

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

Questions?

Summary & Review Day 3

Day 4
Questions related to DAY THREE

Lecture 15
"Drills, Exercises"

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?

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

INTERPRETATION – Drill & Exercise?

- FINLAND - 13.6 ja 13.7 (alusten miehistön sekäyhtiön turvapäälliköiden ja alusten turvapäälliköiden turvaharjoitusten 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).

Drills & Exercises

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

EUROPEAN HANDBOOK OF MARITIME SECURITY EXERCISES AND DRILLS

Definitions

❑**DRILL –** A drill is a small, coordinated practice that tests at least one part of the Port Facility Security Plan (PFSP). A drill is used to test a procedure or a particular function. It serves to maintain a high level of preparedness. Small drills concentrating on a single aspect of the plan are important in training specifically for that aspect.

❑**EXERCISE –** An exercise is an annual activity involving extensive training in which various aspects of the Port Facility Security Plan or Port Security Plan (PSP) are practised. Communication, coordination, availability, resources and reactions are all rehearsed and tested.

❑Large-scale exercises are important for training and testing the coordination between the various components of PFSP /PSP

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.

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

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

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

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.

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

SOME EXERCISES CONDUCTED

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

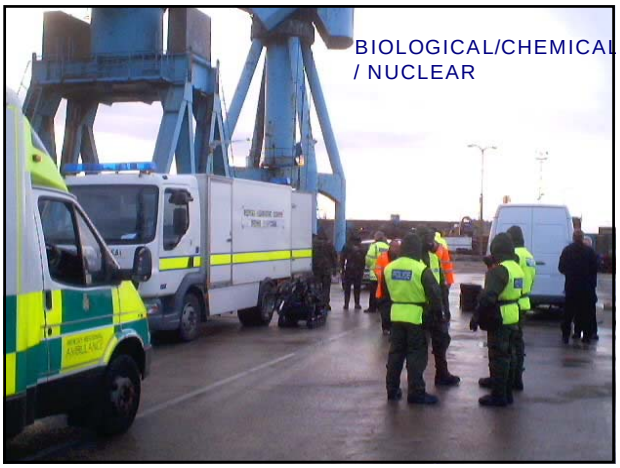
PORT OF LIVERPOOL MAY 2005

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

MULTI AGENCY EXERCISES

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

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

Turkey

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

Questions ?

COFFEE

Lecture 16
"Security Administration"

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 STSTEM

REQUIRED FOR INSPECTION UNDER MSC/CIRC.1151

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

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 2nd & 3rd anniversary
- Renewal verification not exceeding 5 years

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;

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.

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

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".

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

OBLIGATIONS FOR REPORTING SECURITY INCIDENTS

- FOR EACH CONTRACTING GOVERNMENT WHERE IS THIS RESPONSIBILITY PLACED?

RESTRICTED AREA IDENTIFICATION

- EU Regulation "Enhancing Ship and Port Facility Security" provides the mechanism to declare restricted areas. Any such areas should be suitably be identified.
- Signs for;-

- RESTRICTED AREA PERIMETERS
- RESTRICTED AREA ACCESS AND SEARCH POINTS

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.

Reporting to Flag States

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

Questions?

Exercise 5 – CERTIFICATION AND ADMINISTRATION

LUNCH

EXERCISE 6

AUDIT PROCESS

AUDITING & VERIFICATION

- RECALL FROM YESTERDAY;-

Recording and Reporting

- Factual
- Brief
- Identify non conformities
- Not to apportion blame
- Quick to write
- Identify recipient (Master/CSO/SSO?)
- Identifiable to the Audit
- Identify conformance
- Give specific examples

AUDITING PROCESS 2

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

Opening the Audit

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

Non- Conformance 1

- 'Objective Evidence' EU Reg 324:2008
- 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

EXERCISE 6

COFFEE

COURSE ASSESSMENT AND FEEDBACK

Course Objectives

Delegates should on completion of the course will have an understanding of:-

- Legal Framework
- Introduction to the International Legislation on security
- General introduction of the ISPS Code and related background information
- Role of the EU and EMSA
- Need and Scope of ISPS Code related to National Legislation
- Importance of ISPS Code in the supply chain and the concept of intermodel security policy.

Course Objectives Part 2 (S)

- The role, tasks and responsibility of all those involved in the application, operation and control of ISPS Application.
- Operational issues related to ISPS Application

Purpose of the Code

- Thought to be about TERRORISM
- Terrorism not explicitly stated in the Code
- If the measures of the ISPS Code are appropriately applied, provides a mechanism to protect against all security risks.

ISPS Process

- Applied through SOLAS XI-2
- The ISPS Code effective from 1/7/2004
- Application – Regulation 2

SOLAS XI-2

- Regulation 3 – Obligations of the Contracting Government
- Regulation 4 - Requirements for Companies and Ships
- Regulation 5 – Specific Responsibilities of Companies
- Regulation 8 – Masters Authority
- Regulation 9 – Control & Compliance Measures
- Regulation 13 – Communication of Information

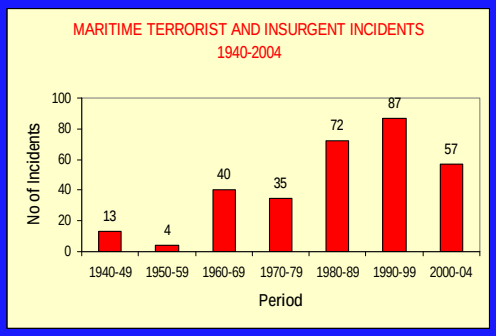
ISPS Code

- PART A – Mandatory
- PART B – Guidance
- 19 Parts

Terrorism / Security

- Terrorism not explicitly considered.
- If effective implementation provides for a comprehensive security regime

International Maritime Attacks

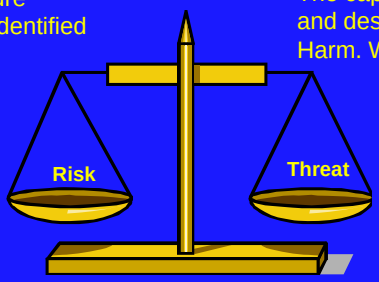


Source – D.McDonald/P.Levey TRANSEC

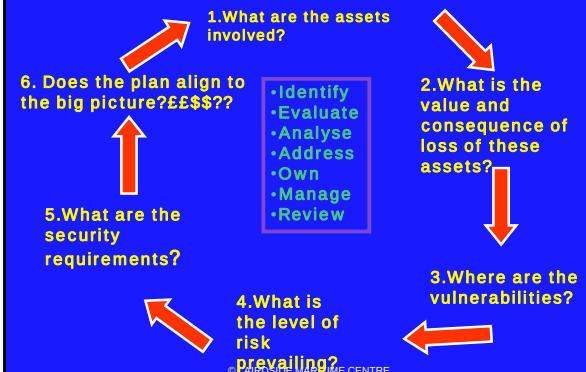
The Balance of Risk and Threat

Exposure to the identified threat

The capability and desire to Harm. Who?



Managing Risks



CODE OF PRACTICE ON SECURITY IN PORTS

IMO/ILO
MESSHP/2003/14
Appendix A - PSA

What is a Ship Security Assessment (SSA)?

The SSA is a process by which competent persons identify key assets on board a ship and assesses the threats to these assets and identifies security measures that can be implemented to reduce the vulnerability of these assets.

THE FIRST STAGE OF COMPLYING WITH ISPS REQUIREMENTS AND MUST BE REVIEWED AS TO IT'S CONTINUING RELEVANCE

SHIP SECURITY ASSESSMENT No. 1

- Assessment will be carried out by Competent persons
  - It is be ship specific.
  - It is be risk based.
  - It is be based on specific threat scenarios
  - It involves an on site survey.
  - It forms the basis of the SSP.
  - The SSA must be protected from unauthorised access or disclosure.
- A Report forms the basis to develop the plan.

SHIP SECURITY PLAN

Purpose Of The SSP

- The SSP is defined in Part A section 2.1 of the ISPS Code and is 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 Section 9

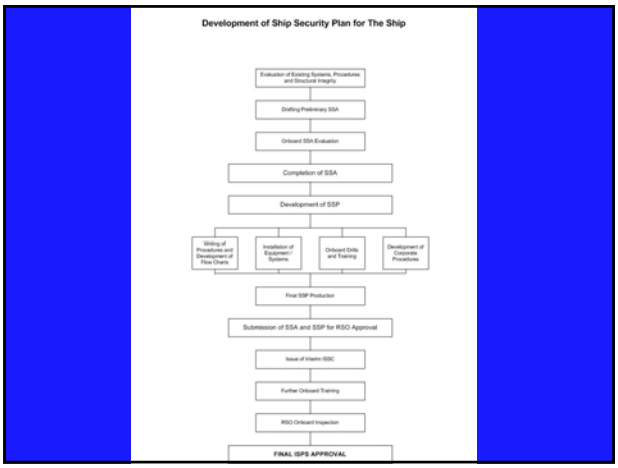
- The SSP is ship specific and based on the SSA
- Confidential and must be retained on board
- Must be approved by the flag administration or RSO
- SSP and the SSA to be submitted to the flag
- Describes security procedures under different levels of security
- Is in the working language of the ship –which if not English, French or Spanish a translation of one of these languages shall be included
- Amendments must be submitted for approval.

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.
- It is useful where the Administration provides guidance of details and measures that must be taken into account and measures that must complied with.
- This allows a consistent application across the administrations ships.

IMPLEMENTATION OF THE SSP

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



ISM CODE & ISPS CODE

INTERNATIONAL MANAGEMENT SAFETY CODE
Revised Guideline – 2002

INTERNATIONAL SHIP & PORT FACILITY SECURITY CODE & SOLAS Amendments 2003

SIMILARITIES AND RELATIONSHIPS BETWEEN SAFETY AND SECURITY

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

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

ISPS CODE RESPONSIBILITIES

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

SHIPPING COMPANIES
IMPLEMENT and MAINTAIN THE SSP. APPOINT and SUPPORT THE CSO, SSO and MASTER

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.
- The Regulation makes selected paragraphs of Part B of the ISPS Code (the guidance section) become mandatory for Member States
- The Regulation also proposes to extend 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.

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

ENGAGEMENT OF RSO's

- When delegating RSO's to carry out work for them Contracting governments should ensure that the RSO has the competencies to undertake the task
- 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

MONITORING & CONTROL

- It is essential that **SSP is** reviewed regularly deficiencies and non conformances noted and improvements implemented
- All Amendments/improvements identified must be submitted to the Contracting Govt for approval before their implementation

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.

Review versus Audit

- Similarities between an Audit and a Review but they are <u>not</u> the same.
- The Review is focused on identifying the suitability of the system.

SECURITY EQUIPMENT

Examples of Security Equipment and Systems

- Locks
- Lighting
- Booms
- Turnstiles/Gates/Barriers
- Fencing and Gates
- Biometric Systems
- Perimeter Intrusion Devices (PIDS)
- Alarms
- Communication systems (Radios)
- Closed circuit TV
- Baggage screening equipment
- Under vehicle video (UVV)
- 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

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

IMO Guidance

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

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 judgement 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);

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.
- Ensure retention of the DoS for inspection
- Records of DoS 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.
- 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.

SOLAS AMENDMENTS

SOLAS V

- **AUTOMATIC IDENTIFICATION SYSTEM, (AIS)**

  AIS TO BE FITTED TO ALL SHIPS >300GT NOT LATER THAN 1ST S.E.C AFTER 1ST 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 1ST RADIO SURVEY AFTER 1ST JULY 2004. CARGO SHIPS > 500GT & MODUs NOT LATER THAN 1ST JULY 2006). *Will have a MINIMUM of Two Activation Points*
- **CONTINUOUS SYNOPSIS REPORT (CSR)**
- **SHIP IDENTIFICATION NUMBER**

  (SEVEN DIGIT NUMBER TO BE MARKED ON HULL EXTERNALLY AND INTERNALLY BY 1ST D/D AFTER 1ST JULY 2004. PASSENGER SHIP > 100GT OTHER SHIPS > 300GT)

SUPPLY CHAIN SECURITY

- Presently there are four main initiatives governing the security of Intermodel Transport:
- 'SAFE FRAMEWORK OF STANDARDS' Initiated by the (WCO) World Customs Organisation, the following two projects implemented to compliment this initiative:
- 'CUSTOMS TRADE PARTNERSHIP AGAINST TERRORISM' Initiated in the U.S. by Customs and Border Protection Department (CBP) this is a voluntary supply chain security programme.
- 'CONTAINER SECURITY INITIATIVE' again introduced by the US (CBP) to increase security of container cargo shipped to them.
- 'AUTHORISED ECONOMIC OPERATOR' To compliment the US efforts E.U. REG 648/2005 and Commission Reg. EEC No 1875/2006 initiated a similar scheme in line with C-TPAT to secure international supply chains in Europe

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

MSC/Circ.1154
T2/4.2 23 May 2005

- **GUIDELINES ON TRAINING AND CERTIFICATION FOR COMPANY SECURITY OFFICERS**

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.

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 DIRECTIVE E.U. 725/2004

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.

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 STSTEM

REQUIRED FOR INSPECTION UNDER MSC/CIRC.1151

Questions?

- THANK YOU FOR YOUR INPUT, SUPPORT AND ENTHUSIASM THROUGHOUT THE COURSE.
- NOW FOR THE ASSESSMENT

A Course prepared for

EMSA

EMSA PRESENTATION

CLOSE COURSE

EMSA

SUMMARY AND CLOSE