THE INTERNATIONAL SHIP AND PORT FACILITY CODE

by

Prof. Pietro del Rosso

ME Lecturer at I.I.S.S. "Amerigo Vespucci" – Molfetta – Italy

and

Mediterranean Training Center Ltd.

KEY WORDS:

- International Ship and Port Facility Security (ISPS) Code
- Mobile Offshore Drilling Units (MODUs)
- Security Alert System
- AIS (Automatic Identification System)
- Ship Security Assessment (SSA)
- Ship Security Plan (SSP)
- Recognized Security Organization (RSO)
- International Ship Security Certificate (ISSC)
- Company Security Officer (CSO)
- Safety Security Officer (SSO)
- Port Facility Security Officer (PFSO)
- Declaration Of Security (DOS)

ISPS CODE

Events in the recent past have proven that no country in the world is safe against terrorists. Terrorist attacks can, for whatever motives, occur at any time and at any place and even the shipping industry cannot escape that fact.

The **International Ship and Port Facility Security Code** (ISPS Code) is a comprehensive set of measures designed to enhance the security of ships and port facilities which has been developed in response to the perceived threats to ships and port facilities in the wake of the 9/11 attacks in the United States.

ISPS BACKGROUND

The hijacking of the Italian cruise ship **Achille Lauro,** in October 1985, marked one of the first actual terrorist acts recorded in modern maritime history. Following that incident, the International Maritime Organization adopted resolution A.584(14) on "*Measures to Prevent unlawful acts which threaten the safety of ships and the security of their passengers and crews*".

This resolution invited the MSC to develop detailed and practical technical measures to ensure the security of passengers and crews on board ships, taking into account the work of the International Civil Aviation Organization in the development of standards and recommended practices for airport and aircraft security.

In 1986, IMO issued MSC/Circ.443 on "*Measures to prevent unlawful acts against passengers and crews on board ships"* providing guidelines on the steps that should be taken, with particular reference to passenger ships engaged on international voyages of 24 hours or more and the port facilities which service them.

In March 1988 a conference in Rome adopted the "*Convention for the Suppression of Unlawful Acts Against the Safety on Maritime Navigation, 1988*" and the "*Protocol for the Suppression of Unlawful Acts Against the Safety of Fixed Platforms Located on the Continental Shelf, 1988*".

In 1996 the MSC adopted MSC/Circ.754 on *Passenger ferry security*.

In the wake of the tragic events of 11 September 2001 in the United States of America, Assembly resolution A.924(22) (November 2001) "*Review of measures and procedures to prevent acts of terrorism which threaten the security of passengers and crews and the safety of ships*", called for a review of the existing international legal and technical measures to prevent and suppress terrorist acts against ships at sea and in port, and to improve security aboard and ashore.
The aim was to reduce risks to passengers, crews and port personnel on board ships and in port areas and to the vessels and their cargoes and to enhance ship and port security and avert shipping from becoming a target of international terrorism.
As a result of the adoption of this resolution, a Diplomatic Conference on Maritime Security, held at the London headquarters of the International Maritime Organization (IMO) from 9 to 13 December 2002, was attended by 109 Contracting Governments to the 1974 SOLAS Convention, observers from two IMO Member States and observers from the two IMO Associate Members. United Nations specialized agencies, intergovernmental organizations and non-governmental international organizations also sent observers to the Conference.
The Conference adopted a number of amendments to the International Convention for the Safety of Life at Sea (SOLAS), 1974, as amended, the most

far-reaching of which enshrined the new **International Ship and Port Facility Security Code (ISPS Code)**.
The ISPS Code entered into force on 1 July 2004 and included detailed security-related requirements for Governments, port authorities and shipping companies in a mandatory section (Part A), together with a series of guidelines about how to meet these requirements in a second, non-mandatory section (Part B). The Conference also adopted a series of resolutions designed to add weight to the amendments, encourage the application of the measures to ships and port facilities not covered by the Code and pave the way for future work on the subject.

REGULATORY FRAMEWORK FOR MARITIME SECURITY

SOLAS chapter XI has been amended to include special measures for maritime security.
Specifically, SOLAS Chapter XI has been divided into two parts:

- Chapter XI-1: “Measures to Enhance Maritime Safety”;
- Chapter XI-2: “Special Measures to Enhance Maritime Security”.

In principle chapter XI-2 incorporates new regulations regarding definitions and the requirements for ships and port facilities. These regulations are supported by the **International Ship and Port Facility Security Code** (ISPS Code) which has a mandatory section (Part A) and a recommendatory section (Part B). The guidance given in Part B of the ISPS Code is to be taken into account when implementing the SOLAS XI-2 regulations and the provisions of Part A.
However, it is recognized that the extent to which the guidance on ships applies depends on the type of ship, its cargoes and/or passengers, its trading pattern and the characteristics of the Port Facilities visited by the ship. Similarly, in relation to the guidance on Port Facilities, the extent to which this guidance applies depends on the types of cargoes and/or passengers and the trading patterns of visiting vessels. In principle, the requirements will be applicable to Mobile Offshore Drilling Units (MODUs) in transit and in port and will not apply to fixed and floating platforms and MODUs on site.

ISPS APPLICATION

In essence, the ISPS Code takes the approach that ensuring the security of ships and port facilities is a risk management activity and that, to determine what security measures are appropriate, an assessment of the risks must be made in each particular case.

The purpose of the ISPS Code is to provide a standardised, consistent framework for evaluating risk, enabling Governments to offset changes in threat with changes in vulnerability for ships and port facilities through determination of appropriate **security levels** and corresponding **security measures**.

The provisions of the ISPS Code apply both to ships and port facilities.

In particular, it applies to the following types of ships engaged on international voyages:

- Passenger ships, including HSC (High Speed Crafts)
- Cargo ships of 500 grt and upwards, including HSC
- Mobile offshore drilling units

It also applies to port facilities serving such ships engaged on international voyages.
The **Security Alert System** as required by SOLAS 74 as amended, Reg. XI-2/6, is also part of the security equipment required under the ISPS Code (in addition to other safety-related items such as the **Automatic Identification System (A.I.S.)**, the ship identification number and the continuous synopsis record).

ISPS CODE SECURITY LEVELS

ISPS Code has identified three security levels 1, 2 or 3 which respectively correspond to a normal, heightened and exceptional threat situation.

Security level 1: normal, the level at which the ship or port facility normally operates. Security level 1 means the level for which minimum appropriate protective security measures shall be maintained at all times.

Security level 2: heightened, the level applying for as long as there is a heightened risk of a security incident.
Security level 2 means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

Security level 3: exceptional, the level applying for the period of time when there is the probable or imminent risk of a security incident.
Security level 3 means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

Setting security level 3 should be an exceptional measure applying only when there is credible information that a security incident is probable or imminent. Security level 3 should only be set for the duration of the identified security threat or actual security incident. While the security levels may change from security level 1, through security level 2 to security level 3, it is also possible that the security levels will change directly from security level 1 to security level 3.

ISPS REQUIREMENTS

The ISPS Code requires a **Ship Security Assessment (SSA)** to be carried out by the company for each ship of its fleet. This SSA should basically include a so-called “on-scene security survey“ and the review of “threat scenarios”. Based on the conclusions of this SSA, particularly the identification of the particular features of the ship and the potential threats and vulnerabilities, a **Ship Security Plan (SSP)** will have to be prepared by the company and submitted for approval by the Flag administration or a **Recognized Security Organization (RSO).**

The ISPS Code also requires relevant personnel to have sufficient knowledge to perform their assigned duties with respect to the relevant provisions of the SSP, to receive adequate training and to carry out drills and exercises.

Another important requirement of the ISPS Code is the provision of specific records of all security activities, which shall be kept on-board.

An **International Ship Security Certificate (ISSC)** shall then be issued to the completion of the initial verification.

COMPANY’S RESPONSIBILITY

EXTRACTS FROM SOLAS XI-2, Reg.5 :

“The company shall ensure that the master has available on board, at all times, information through which officers duly authorised by a Contracting Government can establish :

- *Who is responsible for appointing the members of the crew or other persons currently employed or engaged on board the ship in any capacity on the business of that ship*
- *Who is responsible for deciding the employment of the ship*
- *In cases where the ship is employed under the terms of charter party(ies), who are the parties to such charter party (ies) “*

COMPANY’S OBLIGATIONS

EXTRACTS FROM THE ISPS CODE PART A, paragraph 6 :

“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.”

“ 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”.

COMPANY SECURITY OFFICER (CSO)

Under the terms of the ISPS Code, shipping companies are required to designate a **Company Security Officer (CSO)** and a **Safety Security Officer (SSO)** for each ship.

Among the duties and responsibilities of the CSO are :

- Ensuring sufficient attention and resources are allocated to security and advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information
- Ensuring that the Ship Security Assessment are carried out by persons with appropriate skills to evaluate the security of a ship
- Ensuring the development, submission for approval, implementation and maintenance of the SSP
- Ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship specific information accurately
- Modifying the SSP to correct deficiencies and satisfy the security requirements of the individual ship
- Ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained
- Ensuring adequate security training for personnel responsible for the security of the ship
- Arranging for internal audits and reviews of security activities
- Arranging for the initial and subsequent verifications of the ship by the Flag or the RSO
- Ensuring that deficiencies and non-conformities identified are promptly addressed and dealt with
- Promoting and enhancing security awareness and vigilance
- Ensuring effective communication, co-ordination and implementation of the Ship Security Plan with the SSO and relevant Ports Facility Security Officers(PFSO)
- Ensuring consistency between security requirements and safety requirements

In addition, the CSO may ensure the development, implementation and maintenance of the **Company Security Manual**, if any (not mandatory).
The CSO should therefore have the following documentation for each ship and/or have a working knowledge of the following:

- Updated general layout of each ship of the company
- Location of restricted areas (such as bridge, engine-room, radio-room, steering gear spaces...)
- Location and function of access points (actual or potential) to the ship
- Location of areas that can harbour stowaways or unlawful personnel on-board the ship
- Cargo spaces and stowage arrangements
- Location where unaccompanied baggage is stored
- Locations where the ship's supplies and equipment for ship's maintenance is stored.
- Open Deck arrangements including :

a) height of the deck above water and
b) height to the quay at various levels of the tide and at various stages of cargo loading or unloading.

- Emergency and standby equipment available and stored
- Crew / passenger numerical strength, and security duties of ships crew
- Existing security and safety equipment for the protection of passengers and crew

- Evacuation routes and passenger assembly points (in case of evacuation of the ship)
- Existing security measures and procedures in effect to include monitoring, control, inspections, personnel ID, documents and communications, alarms, lighting, and access control
- Relevant international conventions, codes and recommandations
- Dangerous substances
- Security devices and systems available
- Government legislation and regulations
- Existing agreements with private security companies

SHIP SECURITY OFFICER (SSO)

Among the duties and responsibilities of the **SSO** are:

- Maintaining and supervising the implementation of the SSP on-board (including any amendments to the plan)
- Proposing modifications to the SSP
- Co-ordinating the implementation of the SSP with the CSO and the relevant PFSO
- Carrying out regular security inspections of the ship to ensure appropriate security measures are maintained
- Co-ordinating the security aspects of the handling of cargo and ship's stores with other crew and the relevant **Port Facility Security Officer (PFSO)**
- Promoting security awareness and vigilance among the crewmembers
- Reporting all security incidents
- Ensuring adequate crew training is carried out
- Ensuring that security equipment is properly operated, tested, calibrated and maintained
- Reporting to the CSO any deficiencies and non-conformities and implementing any corrective actions on-board

In addition, the Company may appoint the SSO to review and complete the **Declaration Of Security (DOS)** agreement.

SHIP SECURITY ASSESSMENT (SSA)

The **SSA (Ship Security Assessment)** is to be carried out before developing the **Ship Security Plan (SSP)** and is a major element in the process of developing or updating the SSP.
It is the responsibility of the CSO to ensure that the SSA is carried out by persons with appropriate skills, for each ship in the Company fleet.
The SSA shall include the following steps :
- Identification of key shipboard operations
- Identification of existing security measures and procedures
- Identification of potential threats (threat scenarios)
- Performance of an on-scene security survey
- Identification of weaknesses in both the infrastructure and in the procedures

SHIP SECURITY PLAN (SSP)

Each ship shall carry on-board a SSP which must have been approved by the Administration.
This SSP shall be developed by the company, mainly based on the conclusions of the SSA.
The SSP shall include a clear statement emphasizing the Master's overriding authority and responsibility with respect to the security of the ship.
The plan shall include a list of security measures based on each security level (1, 2 and 3).
The security measures shall cover, as an example, the following items (but are not limited to) :

- General requirements for security of the ship (ensuring the performance of all ship security duties)
- Monitoring of restricted areas to ensure that only authorized persons have access
- Controlling access to the ship
- Monitoring of deck areas and areas surrounding the ship
- Controlling the embarkation of persons and their effects
- Supervising the handling of cargo and ship's stores
- Ensuring that port-specific security communication is readily available

The plan shall also address procedures for:

- Training, drills and exercises
- Reporting
- Internal audits and reviews
- Maintenance, calibration and testing of security equipment
- Handling the interface with the port facility (ref : DOS)
- Handling the ship security alert system (testing, activation, deactivation, resetting)

The SSP shall also, in addition, include contingency procedures, which have to be followed in unusual circumstances that present a threat to the security of the ship.

TRAINING OF CSO, SSO AND RELEVANT SHORE-BASED PERSONNEL

CSO, SSO and the relevant shore-based personnel shall have knowledge and have received training on the relevant security matters.
The relevant shipboard personnel engaged on specific security tasks shall have sufficient knowledge to carry out the specific security duties by means of training, drills and exercises.
Additional training of SSO may include :

- The layout of the ship
- The SSP and related procedures (including scenario-based training on how to respond)
- Crowd management and control techniques
- Operations of security equipment and systems

- Testing, calibration and whilst at sea maintenance of security equipment and systems

INTERNAL AUDITS/REVIEWS

The CSO and the SSO shall ensure that internal audits of the security system and reviews of the approved SSP are duly carried out.
The personnel conducting the internal audits must be specified in the SSP.
It shall also be independent of the activities being audited, unless this is impracticable.

GUIDANCE

The company may develop internal procedures and "Shipboard Security Inspection" checklists, although this is not required by the Code.
As an example, the company may require, in its internal procedures that an audit of the security system is carried out on-board each ship of the company's fleet, and duly reported, with any non-conformities and corrective or preventive action in an "audit report".
If the company has developed a **Company Security Manual** (not mandatory), then this manual may also include a company audit programme.

CONCLUSIONS

While the ISPS Code lays out procedures to be followed, it also provides some recommendations to be observed by everyone such as:

- The capacity to clearly identify personnel visiting the ship;
- The need for a thorough shipment documentation for cargo, stores and equipment being brought aboard;
- Advance notification of the warning for both ship and port, of the arrival of personnel and equipment.

Therefore, the ISPS Code has been successful in the raising of the awareness level of the maritime community on issues of maritime security.
This is a step in the right direction, noting that the goal of the IMO is '*to create the necessary security culture and raise our defences so high that the shipping industry does not become a target for terrorist activities'.*

REFERENCES

- "Introduction to the International Ship & Port Facility Security Code (The ISPS Code)", IMCA, January 2007
- "The European Training Manual for Maritime Security Personnel/ISPS Code", COESS, 2008
- "Maritime Security: Implementation of the ISPS Code" by Chris Trelawny, Senior Technical Officer, Maritime Safety Section, Maritime Section Division, IMO, 2005