Maritime Security

Maritime Security Overview

Aris Klempetsanis/ Senior Project Officer

Visits and inspections

Lisbon 18-19 July 2017

Overview

FRAMEWORK (IMO and EU legal instruments)

IMPLEMENTATION

REQUIRMENTS

CONTROL

FRAMEWORK

IMO legal Instruments

- SOLAS Chapter XI-2, Special measures to enhance maritime security;
- ISPS Code

SOLAS Chapter XI-2

- Regulation XI-2/2: enshrines the ISPS Code.
- Regulation XI-2/3: Administrations shall set security levels and ensure the provision of security level information to ships entitled to fly their flag;
- Regulation XI-2/6: requires all ships to be provided with a Ship Security Alert System (SSAS);
- Regulation XI-2/9 control of ships on maritime security;
- Regulation XI-2/10 covers requirements for port facilities.

ISPS Code

A comprehensive set of measures to enhance the security of ships and port facilities

Part A: Mandatory

Part B: Guidance

ISPS Code/Application

The ISPS Code applies to the **following types of ships** engaged on international voyages :

- passenger ships, including high-speed passenger craft;
- cargo ships, including high-speed craft, of 500 gross tonnage and upwards;
- mobile offshore drilling units; **and**
- **the port facilities serving such ships.**

SOLAS/Additional measures

- Modifications to SOLAS Chapter V/19 (AIS);
- A new regulation XI-1/5 (CSR);
- Regulation XI-I/3 (Ship identification number to be permanently marked in a visible place).
- Long Range Identification and Tracking system (LRIT)

Who has to comply with the ISPS Code?

IMPLEMENTATION

- The ISPS Code is part of SOLAS, so compliance is mandatory for the 148 Contracting Parties to SOLAS Convention.

- When a Government accepts and ratifies an IMO Convention it agrees to make it part of its own national law and to enforce it just like any other law.

- The Contracting Governments are obliged to address all the objectives and functional requirements of SOLAS/XI-2 and of the ISPS Code.

Penalties

What if Contracting governments do not comply?

Penalties?

Penalties

- IMO does not impose any penalties;
- IMO was established to adopt legislation;
- The responsibility for implementation lies with the Contracting governments.

EU Legislation on Maritime Security

1. Regulation (EC) No.725/2004 on enhancing ship and port facility security;

2. Directive 2005/65EC on enhancing port security;

3. Commission Regulation (EC) No.324/2008 on procedures for conducting Commission inspections in the field of maritime security;

Regulation (EC) No.725/2004

- Mandatory certain provisions of ISPS Code Part B;
- Application of security requirements to domestic shipping;
- Designation of a Competent authority for maritime security;
- Designation of a Focal point;
- National programme for maritime security;
- Sanctions;
- COM inspections.

Commission Regulation (EC) No.324/2008

Procedures for conducting Commission inspections in the field of maritime security:

- Administrations;
- Port facilities;
- Ships;
- Companies;
- RSOs.

Directive 2005/65EC on enhancing port security

The main objective of the Directive is to introduce community measures to enhance port security in the face of threats of security incidents.

- **Port security assessments (PSA)**
- **Port security plans (PSP)**
- **Port security officer (PSO)**

REQUIREMENTS

- ADMINISTRATIONS
- COMPANIES
- SHIPS
- PORTS-PORT FACILITIES

ADMINISTRATIONS

- Designation of national authorities responsible for implementation of maritime security;
- Deciding national requirements for maritime security;
- Setting and communication of SL;
- Designation of authorities receiving SSAS alerts;
- Approval of SSP; →
- Verification-Certification of ships;

ADMINISTRATIONS

- Approval of PFSA-PFSP;
- Monitoring of Recognised Security Organisation (RSO), when delegating maritime security tasks;
- **Control:** All 148 Parties to SOLAS must ensure their ships and port facilities comply with the requirements.

COMPANIES

- Appoint a Company Security Officer (CSO);
- Establish the master's overriding authority in the SSP;
- Provide to their ships all means necessary for implementation of security measures;
- Make available to the Master information through which duly authorized officers by a contracting government can establish:
  - Who is responsible for appointing the crew;
  - Who is responsible for the employment of the ship;
  - Who are the parties in case of a charter party.
- Ensure their ships are certified in accordance with ISPS requirements.

SHIPS

- Ship Security Assessment;
- Security Plan;
- Ship Security Alert System;
- Verifications
  - Initial, Intermediate, Renewal, Additional
  - ISSC
- Ship Security Officer;
- RSOs

SHIP SECURITY ASSESSMENT (SSA)

The ship security assessment is an essential and integral part of the process of developing and updating the ship security plan.

The SSA shall include at least, the following elements:

- **Identification of existing security measures, procedures and operations;**
- **Identification and evaluation of key shipboard operations that it is important to protect;**
- **Identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and**
- **Identification of weaknesses, including human factors, in the infrastructure, policies and procedures.**

SHIP SECURITY ASSESSMENT (SSA)

Ship security assessment aims to answer these five questions.

1. **Is there any motive to attack the ship?**
2. **Which are the key shipboard operations and areas that are prone to security incident?**
3. **Are there any existing security measures, procedures in place?**
4. **What are ways ship can be attacked?**
5. **What are the likelihood and consequences of such attack?**

Ship Security Plan (SSP)

Each ship shall carry on board a ship security plan approved by the Administration (ISPS A/9.1)

Ship Security Plan (SSP)

Minimum requirements for the SSP (ISPS 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;

Ship Security Plan (SSP)

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;

Ship Security Plan (SSP)

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;

7. Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;

Ship Security Plan (SSP)

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;

Ship Security Plan (SSP)

12. Procedures for reporting security incidents;

13. Identification of the ship security officer;

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;

Ship Security Plan (SSP)

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 alerts1.

VERIFICATION-CERTIFICATION

VERIFICATION-CERTIFICATION

VERIFICATION-CERTIFICATION

- INITIAL
- RENEWAL
- INTERMEDIATE
- ADDITIONAL

DURATION AND VALIDITY OF CERTIFICATE

- An ISSC shall be issued, after the initial or renewal verification by the Administration or by an RSO acting on behalf of the Administration;

- ISSC shall be issued for a period specified by the Administration which shall not exceed five years;

- Duration and validity ISPS A/19.3.

DURATION AND VALIDITY OF CERTIFICATE

ISSC ceases to be valid in the following cases (ISPS A/19.3.8):

- If the relevant verifications are not completed within the periods specified by ISPS Code (Initial, intermediate, renewal);
- If the Certificate is not endorsed in accordance with section 19.1.1.3 and 19.3.7.1, if applicable;
- When a Company assumes the responsibility for the operation of a ship not previously operated by that Company; and
- Upon transfer of the ship to the flag of another State.

Interim International Ship Security Certificate (IISSC)

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. A Company assuming the responsibility for the operation of a ship not previously operated by that Company until the Certificate referred to in section ISPS A/19.2 is issued.

VERIFICATION - CERTIFICATION

- The tasks of Verification – Certification of ships can be delegated to RSOs;
- The Administration has to monitor their activity;
- The responsibility always lies with the Administration.

PORT FACILITIES

- PFSA
- PFSP
- PFSO

PORT FACILITY SECURITY ASSESSMENT (PFSA)

- Essential and integral part of the process of developing and updating the PFSP.
- Shall be carried out by the Contracting Government.
- A Contracting Government may authorize a RSO to carry out the PFSA.
- The security assessment shall be reviewed and **approved** for compliance with part A of ISPS Code by the Contracting Government.

PORT FACILITY SECURITY ASSESSMENT (PFSA)

ISPS A/15.5 specifies the minimum elements should be included in the PFSA

Port Facility Security Plan (PFSP)

- **Shall be developed on the basis of a port facility security assessment for each port facility;**

- **Shall be approved by the Contracting Government .**

ISPS A/16.3

Minimum requirements for a PFSP

CONTROL

1. PORT FACILITIES

2. FLAG SHIPS (FSI)

3. FOREIGN FLAG SHIPS (PSC-DAO)

- In port
- Intending to enter the port

PORT FACILITIES (control)

There is no standard and common control system in place for port facilities.

FLAG SHIPS

States have the primary responsibility to have in place an adequate and effective system to exercise control over ships entitled to fly their flag, and to ensure that they comply with relevant international rules and regulations in respect of maritime safety, security and protection of the maritime environment.

IMO Resolution A.973(24)

CONTROL AND COMPLIANCE MEASURES

SOLAS regulation XI-2/9

- Control of ships in port;
- Control of ships intending to enter the port.

SANCTIONS

SANCTIONS

“Member States shall ensure that effective, proportionate and dissuasive sanctions for breaching the provisions of this Regulation are introduced”.

Article 14 of Regulation 725/2004

emsa.europa.eu

twitter@emsa_lisbon

facebook@emsa.lisbon

EMSA