

ISPS Code

(International Ship and Port Facility Security Code)

by

Capt Thomas J. Proctor

History

- Initiated by USCG following 9/11 incident.
- Adopted by the International Maritime Organisation (IMO) in 2002 for implementation 01.07.04
- Enshrined in Safety of Life at Sea (SOLAS) XI – 2.

Objective

The objectives of this code are to establish an International framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect/assess security threats and take preventative measures against security incidents affecting ships and or port facilities used in International Trade

Application

The Code Applies to:

- The following types of ships on international voyage
 - Passenger ships, including high-speed craft
 - Cargo ships, including high speed craft, of 500 gross tonnage and upwards
 - Mobile offshore drilling units
- Port facilities serving such ships engaged on International voyages

Code Construction

- **Part A** – Mandatory requirements regarding the provisions of Chapter XI-2 of the Annex to the International Convention for the **Safety of Life at Sea (SOLAS)1974** as amended.
- **Part B** – Guidance regarding the provision of Chapter XI-2 of the Annex to the International Convention for the **Safety of Life at Sea (SOLAS)1974** as amended and Part A of this Code.

Security Levels

- **Security Level 1** means the level for which minimum appropriate security measures shall be maintained at all times.
- **Security Level 2** means the level for which appropriate additional security measures shall be maintained for a period of time as a result of heightened 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 might not be possible to identify the specific target.

PFSA AND PFSP PROCESS

* RISK = THREAT x VULNERABILITY x CONSEQUENCE

TRANSEC guidance offered

UK Port Facilities identified from Industry Groups, Registers and Directories

Security questionnaires sent by TRANSEC to all Port Facilities

TRANSEC check questionnaire and categorise Port Facilities according to traffic type

PFSA programme prioritised by RISK *

PFSA undertaken by TRANSEC security Inspectors in liaison with port management

Site specific PFSA report + PFSI + PFSP template issued to Port Facility

Port Facility completes a PFSP and returns to TRANSEC within 2 months

PLAN APPROVED

NO

YES

Notified to IMO

VERIFICATION & COMPLIANCE INSPECTIONS COMMENCE

Appoint, train and subject PFSO to security vetting

If PFSP is amended after initial approval or if the traffic handled by the port facility changes TRANSEC may require the PFSA process to be repeated

SOURCE TRANSEC

The Initiating Process

- The process in the UK for Ports meeting the obligations for ISPS compliance is different than ships (Recognised Security Organisations) in that it is the duty of the Contracting Govt. (TRANSEC in this case), to undertake the Assessment.
 1. The Port Facility completes a security Questionnaire.
 2. TRANSEC undertake an on scene inspection
 3. The Port is classified - COG - Chemical Oil Gas in this case
 4. A detailed report is produced by TRANSEC and the Port facility is issued with this in addition to the Port Facility Security Instruction for COG Facilities.

Facility Process

1. The Port Facility must then produce a Port Facility Security Plan to address the requirements.
2. A permanent employee of the Port must be nominated as a Port Facility Security Officer who is responsible for establishing the plan and seeking approval.
3. Before acceptance, the PFSO must be trained on a TRANSEC Approved PFSO Course and undergo a successful Counter Terrorist Check.
4. In the interim, all Port facility staff must be appropriately trained.
5. The Plan is then submitted for approval to TRANSEC.
6. Validation testing then taken.

The Plan (PFSP)

1. Introduction
2. Operational Overview & Port Management
3. Assets
4. Threat Assessment
5. Vulnerabilities
6. Counter Measures
7. Conclusion

Assets

- **ASSETS** - Identification and evaluation of important assets & infrastructure it is important to protect
- The table below helps identify key assets and infrastructure vital for the continuation of core business. How important are the following assets and/or infrastructure to the Port's day-to-day business:

Threat Assessment

- **THREAT ASSESSMENT** - Identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritise security measures
- The threat to UK maritime interests and shipping in UK waters at the time of the PFSA was MODERATE. This reflects the absence of any specific, credible indication of terrorist attack planning against the maritime sector. A table of potential threats (including those based on criminal activity) is shown below:

Vulnerabilities

- **VULNERABILITIES** – Identification of weaknesses, including human factors, in the infrastructure, policies and procedure.
- This table outlines vulnerabilities identified with current security counter measures considered. A description of the vulnerabilities should be set out below in the table where appropriate. Considering the likelihood of sabotage, vandalism, theft or other deliberate acts, how vulnerable are the following assets / infrastructure?

COUNTER MEASURES

- COUNTER MEASURES - Identification, selection and prioritisation of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability