What is ISPS Code

The International Ship and Port Facility Security Code

A-M CHAUVEL - BUREAU VERITAS - DNS / DCO
- To establish an international framework to detect security threats and take preventive measures against security incidents affecting ships and port facilities used in INTERNATIONAL TRADE.

- To establish the respective roles and responsibilities of all parties concerned at the national and international level for ensuring MARITIME SECURITY.
ISPS CODE Risk Management for Ships

Requirements include:

- Ship Security Plans
  SSP
- Ship Security Officers
  SSO
- Company Security Officers
  CSO
- Onboard equipment.
ISPS CODE Risk Management for Port facilities

Requirements include:

- Port Security Plans (PSP)
- Port Facility Security Officers (PFSO)
ISPS CODE Risk Management for Port facilities & Ships

Requirements include:

- Monitoring & controlling access
- Monitoring the activities of people and cargo
- Ensuring security communications.
Part A is mandatory

Requirements included in Chapter XI-2 of the International Convention SOLAS

Part B is a Guidance but may become mandatory
ISPS CODE Part A - Mandatory Requirements

1 - General
2 - Definition
3 - Application
4 - Responsibilities of Contracting Governments
5 - Declaration Of Security (DOS)
6 - Obligations of the Company
7 - Ship security
8 - Ship Security Assessment
9 - Ship Security Plan
10 - Records

Apply to Ship
Apply to Ship and Port facility
ISPS CODE Part A - Mandatory Requirements

11 - Company Security Officer
12 - Ship Security Officer
13 - Training, drills and exercises on ship
14 - Port Facility Security
15 - Port Facility Security Assessment
16 - Port Facility Security Plan
17 - Port Facility Security Officer
18 - Training, drills and exercises on port facility
19 - Verification and certification for ship

Apply to Ship
Apply to Port facility
- Gathering and assessing information with respect to security threats

- Requiring the maintenance of communication protocols for ships and port facilities

- Preventing unauthorised access to ships, port facilities and their restricted areas

- Preventing the introduction of unauthorised weapons, incendiary devices or explosives to ships or port facilities
ISPS CODE FUNCTIONAL REQUIREMENTS

- Providing means for raising the alarm in reaction to security threats or security incidents

- Requiring ships and port facility security plans based upon security assessments

- Requiring training and drills to ensure familiarity with security plans and procedures
SHIP SECURITY PLAN

A plan to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship’s stores or the ship from the risks of a security incident.
A plan to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship’s stores within the port facility from the risks of a security incident.
The person on board the ship accountable to the master for security of the ship, including implementation and maintenance of the Ship Security Plan and for liaison with the Company Security Officer and the Port Facility Security Officers.
The person ashore designated by the company for ensuring that a ship security assessment is carried out, that the Ship Security Plan is developed, approved, implemented and maintained and for liaison with Port Facility Security Officer and the Ship Security Officer.
The person appointed as responsible for the development, implementation, revision and maintenance of the Port Facility Security Plan and for liaison with the Ship Security Officers and the Company Security Officers.
ISPS CODE IS APPLICABLE TO:

- Passenger ships, including passenger high-speed craft

- Cargo ships, including high-speed craft of 500 gross tonnage and upwards

- Mobile offshore drilling units

- Port facilities serving ships engaged on international voyages
Contracting Governments shall set **security levels** and provide **guidance** for protection from security incidents.
Contracting Government must conduct port facility security assessments based on risk:

- Criticality
- Threat
- Vulnerability
- Identification and evaluation of important assets and infrastructures that are critical to the port facility if damaged

- Identification of the actual threats to those critical assets and infrastructure in order to prioritise security measures

- Identification of the port facility in term of vulnerability and other areas within a port that may be a likely target
Once this assessment has been completed, the Contracting Government can evaluate risk:

\[ \text{Risk} = C \times T \times V \]
RESPONSIBILITIES OF CONTRACTING GOVERNMENTS

Factors to be considered in setting appropriate security level:

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
4. The potential consequences of such security incident
Contracting Governments shall determine when a Declaration Of Security is required by assessing the risk the ship / port interface or ship to ship activity poses to people, property or the environment.
A ship can request completion of a Declaration Of Security when:

1- The ship is operating at a **higher security level** than the port facility or another ship it is interfacing with.

2- There is **an agreement** on the declaration of security between Contracting Governments covering certain international voyages or specifics ships on those voyages.

3- There has been a **security threat or a security incident** involving the ship or the port facility, as applicable.

4- The ship is at port which is **not required** to have implemented an approved port facility security plan.

5- The ship is conducting ship to ship activities with another ship **not required** to have and implement an approved ship security plan.
The Declaration Of Security is valid from xx/xx/20xx to xx/xx/20xx for the following activities:
...

Under the following security levels
Security level(s) for the ship:
...

Security level(s) for the port facility:
...

Signed for and on behalf of
The Port Facility
The Ship
<table>
<thead>
<tr>
<th>Activity</th>
<th>PFSO Port</th>
<th>SSO Ship</th>
</tr>
</thead>
<tbody>
<tr>
<td>Ensuring the performance of all security duties</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring restricted areas to ensure that only authorized personnel have access</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controlling access to the port facility</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controlling access to the ship</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Monitoring of the port facility, including berthing areas and areas surrounding the ship</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handling of cargo</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Delivery of ship’s stores</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Handling unaccompanied baggage</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Controlling the embarkation of persons and their effects</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Ensuring that security communication is readily available between the ship and the port facility</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
The Declaration Of Security shall be completed by:

- The Master or the Ship Security Officer on behalf of the ship.

- The Port Facility Security Officer or, if the Contracting Government determines otherwise, by another body responsible for shore-side security, on behalf of the port facility.

- The Declaration Of Security shall address the security requirements that should be shared between a port facility and a ship or between ships.

- Administration shall specify the minimum period for which Declarations Of Security shall be kept by ships entitled to fly their flag.
OBLIGATIONS OF THE COMPANY

The company shall ensure that the Ship Security Plan contains:

- Clear statement emphasising the Master’s authority

- Master overriding authority and responsibility to make decisions with respect to the security of the ship

- Request the assistance of the company or of any Contracting Government as may be necessary

The Company Security Officer, the Master and the Ship Security Officer shall be given the necessary support to fulfil their duties and responsibilities.
SHIP SECURITY

- Ship is required to act upon the security levels set by Contracting Government

- In order to communicate the threat at port facility or for the ship, the Contracting Government sets the appropriate security level:

Level 1 : Low threat situation
Level 2 : Medium threat situation
Level 3 : High threat situation
SHIP SECURITY at LEVEL 2 & 3

- The ship shall acknowledge receipt of the Administration’s or of the Contracting Government’s instructions on the change of security level.

- The ship shall confirm to the Port Facility Security Officer the initiation of the implementation of the appropriate measures and procedures as details in the Ship Security Plan and report any difficulties in implementation.

- If the ship is required to set, or is already at a higher level than set for the port it intends to enter, the ship shall advice the designated authority and the Port Facility Officer of the situation. In such cases, the Ship Security Officer shall liaise with the Port Facility Security Officer and co-ordinate appropriate actions, if necessary.
SHIP SECURITY ASSESSMENT (SSA)

The SSA is an essential and integral part of the process of developing and updating the Ship Security Plan. The Company Security Officer shall ensure that the SSA is carried out by persons with appropriate skills to evaluate the security of the ship.
The SSA shall include an on-scene security survey and, at least, with identification of:

1 - Existing security measures, procedures and operations

2 - Evaluation of key ship board operations that it is important to protect

3 - Possible threats to the key ship board operation

4 - Weakness, including human factors in the infrastructure, policies and procedures

The SSA shall be documented, reviewed, accepted and retained by the company.
SHIP SECURITY ASSESSMENT (SSA)

Address the following elements on board or within the ship:

Personnel protection systems

Physical security

Procedural policies

Structural integrity

Radio, telecommunication, computer systems

Other areas that may, if damaged or used for illicit observation, pose a risk to...
SHIP SECURITY ASSESSMENT ( SSA )

Should consider the persons, activities, services and operations that it is important to protect. This includes:

1- Ship’s personnel
2- Passengers, visitors, vendors, repair technicians, port facility personnel
3- Capacity to maintain safe navigation and emergency response
4- Cargo, particularly dangerous goods or hazardous substances
5- Ship’s stores
SHIP SECURITY ASSESSMENT ( SSA )

On-scene security survey should examine and evaluate existing shipboard protective measures, procedures and operations for:

1- Ensuring the performance of all ship security duties
2- Monitoring restricted areas to ensure access only to authorised persons
3- Controlling access to the ship, including any identification systems
4- Monitoring of deck area and area surrounding the ship
5- Controlling the embarkation of persons and their effects
6- Supervising the handling of cargo and the delivery of ship’s store
7- Ensuring that ship security communication, information, and equipment are readily available
RISK MATRIX

PEOPLE
ASSETS
ENVIRONMENT
COMPANY IMAGE

Extremely Remote
Remote
Probable
Frequent
Very Frequent

Minor
Moderate
Major
Severe
Catastrophic

Manage for continuous improvement
Incorporate risk reduction measures
Intolerable

Minor
Slight impact
National impact
International impact
Continued Int. impact
Determine if the scenario requires a mitigation strategy

Select a scenario

Evaluate the scenario in terms of the vessel’s vulnerability

Evaluate the scenario in terms of the potential consequences

Implement mitigation strategy (protective measures)
SHIP SECURITY PLAN ( SSP )

Each ship shall carry on board a SSP approved by the Administration

- The plan shall make provisions for the three security levels.


- The plan shall be written in the language or languages of the ship.

- Submission of ship plans, or amendments, for approval shall be accompanied by the Ship Security Assessment on the basis of which the plan, or amendments, have been developed.
SHIP SECURITY PLAN (SSP)

The SSP shall consist, at least, of:

1- Prevent weapons, dangerous substances and devices intended to use against people, ships or ports

2- Identification of the restricted areas and measures for the prevention of unauthorised access

3- Prevention of unauthorised access to the ship

4- Responding to security threats or breaches of security

5- Responding to security instructions given by Contracting Governments at security level 3

6- Evacuation in case of security threats or breaches of security
SHIP SECURITY PLAN ( SSP )

The SSP shall consist, at least, of:

1. Duties of shipboard personnel assigned security responsibilities
2. Auditing the security activities
3. Training drills and exercises
4. Interfacing with port facility security activities
5. Periodic review of the plan for updating
6. Reporting security incidents
7. Identification of the Ship Security Officer
SHIP SECURITY PLAN ( SSP )
The SSP shall consist, at least, of:

14- Identification of the company security officer including 24-hour contact details

15- Inspection, testing, calibration and maintenance of security equipment

16- Frequency of testing or calibration any security equipment provided on board

17- Identification of the locations where the ship security activation points are provided

18- Procedures, instructions and guidance on the use of the ship security alert system including testing, deactivation and resetting and to limit false alerts
Changes to the Ship Security Plan shall not be implemented unless approved by the Administration.

- The records may be kept in electronic format. In such case they shall be protected by procedures aimed at preventing their unauthorised deletion, destruction or amendment.

- The plans shall be protected from unauthorised access or disclosure.
SHIP SECURITY PLAN (SSP)

1 - Detail the organisational structure of the security for the ship
2 - Detail the ship’s relationships with company and port facilities, other ships and relevant authorities with security responsibility
3 - Detail the communication system to allow effective communication within the ship & between the ship and others, including the port facilities
4 - Detail the basic security measures for security level 1
5 - Detail the additional security measures that will allow the ship to progress without delay to security level 2 or 3
6 - Provide for regular review, or audit, and for its amendment
7 - Reporting procedures to the appropriate Contracting Governments contact points.
SHIP SECURITY PLAN (SSP)

Areas where security measures could be taken:

- Access to the ship
- Restricted areas
- Monitoring the security of the ship
- Delivery of ship’s stores
- Handling of cargo
- Handling unaccompanied baggage
<table>
<thead>
<tr>
<th>Protective Measures</th>
<th>Level 1</th>
<th>Level 2</th>
<th>Level 3</th>
</tr>
</thead>
<tbody>
<tr>
<td>Access points are normally secured(©) or continuously attended to prevent unauthorized access</td>
<td>YES</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Weather-deck access vents, storage lockers, and doors to normally unmanned spaces (such as storerooms, auxiliary machinery rooms, etc) may be locked (©) or precautions taken to prevent unauthorized access</td>
<td></td>
<td>YES</td>
<td></td>
</tr>
<tr>
<td>Limit entry to the level to a minimum number of access points (While not restricting egress from the vessel in the event of an emergency)</td>
<td>Optional</td>
<td>YES</td>
<td>YES*</td>
</tr>
<tr>
<td>Coordinate with the waterfront facility to extend access control beyond the immediate area of the vessel</td>
<td>Optional</td>
<td></td>
<td>YES</td>
</tr>
</tbody>
</table>

© Doors in escape routes must be capable of being opened without keys from the direction for which escape is required.

* Limit entry to to a single access point

Source: NVIC 10 02 - US Coast Guard
RECORDS

Records of the following activities shall be kept on board for at least the minimum period *specified by the Administration*:

1. Training, drills and exercises
2. Security threats & incidents
3. Breaches of security
4. Change in security level
5. Communications relating to the direct security of the ship
6. Internal audit and review of security activities
7. Periodic review of the ship security Assessment
8. Periodic review of the ship security plan
Records of the following activities shall be kept on board for at least the minimum period specified by the Administration:

9- Implementation of any amendments to the plan

10- Maintenance, calibration and testing of security equipment and ship security alert system

The records shall be protected by procedures aimed at preventing their unauthorised deletion, destruction or amendment.

The records shall be protected from unauthorised access or disclosure.
The **Company Security Officer** and appropriate **shore-based personnel** and the **Ship Security Officer** shall have knowledge and receive training. 

**Shipboard personnel** having specific security duties and responsibilities shall have sufficient knowledge and ability to perform their assigned duties.

Drills and exercises shall be conducted at appropriate intervals taking into account the ship type, **ship personnel changes**, port facilities to be visited and other relevant circumstances.

The **Company Security Officer** shall ensure the effective co-ordination and implementation of the SSP by participating in exercises at appropriate intervals.
TRAINING DRILLS & EXERCISE on SHIP SECURITY

Frequency:

At least once every
three months

But in case where more than 25% of the ship’s personnel has been changed within the last three months, a drill should be conducted within one week of the change.
At least once every calendar year with no more than 18 months between the exercises.

**WHO**

- CSO
- PFSO
- Relevant authority of Contracting Government
- SSO

**WHAT**

- Communications
- Co-ordination
- Resource availability
- Response