

## **International Ship & Port Facility Code (ISPS) What it is exactly – and what is it meant to do?**

In the wake of 9/11 the IMO - International Maritime Organization (in December 2002), adopted new Regulations to enhance maritime security through amendments to the SOLAS Convention - Chapters V and XI.

Chapter XI, that previously covered ship safety and security, has been split into two new chapters, XI-1 and XI-2.

Chapter XI-1, the “Special Measures to Enhance Maritime Safety” has been enhanced to include additional requirements covering ship identification numbers and carriage of a Continuous Synopsis Record.

Chapter XI-2, the “Special Measures to Enhance Maritime Security” has been created and includes a requirement for ships and companies to comply with the International Ship and Port Facility Security (ISPS) Code.

Port Security compliance with the ISPS International Ship & Port Facility Code (ISPS) comes into effect on 1 July 2004.

There are a few provisions within the Code that have a different implementation date.

There are two parts to the ISPS Code - Part A and Part B.

Part A covers mandatory requirements.

Part B covers guidance.

Some national governments intend to make Part B compulsory.

The USCG has decreed that sections of Part B of the Code will also be taken into consideration.

Chapter XI-2 sets out requirements for ship security alert systems and control and compliance measures for port states and contracting governments.

As well as the new Regulations in SOLAS Chapter XI-2, the IMO has adopted amendments to extant SOLAS Regulations accelerating the implementation of the requirement to fit automatic identification systems (AIS) (Chapter V). The IMO has also adopted a number of Conference Resolutions including technical co-operation, and the co-operative work with the International Labour Organization and World Customs Organization.

Review and amendment of certain of the new provisions regarding maritime security may be required on completion of the work of these organizations.

These requirements form a framework through which ships and port facilities can co-operate to detect and deter acts, which pose a threat to international maritime security.

.....  
The regulatory provisions of the ISPS Code do not extend to the actual response to any given security incident, nor do they extend to any necessary clear-up activities after such an incident.  
.....

**The ISPS Code was designed to:**

1. Address international maritime security concerns on terrorism, post 9/11.
2. Ensure that international acceptable standards and security measures are in place.
3. Enhance the ability of Sovereign Nations to detect and/or deter security threats within an international framework.
4. Establish clear and identifiable roles and responsibilities for doing so.
5. Provide a platform for the collection and exchange of security intelligence.

**It requires ship and port facility staff to:**

1. Check that compliance with international security standards are in place.
2. Address the ISPS Code international security standards if they are not.
3. Restrict access; prevent the introduction of unauthorized weapons, etc.
4. Ensure the means to raise necessary alarms are in place.
5. Ensure all Vessels and Port Authorities have security plans.
6. Ensure Port Facility and Vessel Security training and drills are conducted.
7. Collect / assess / disseminate intelligence information.
8. Maintain all international communication protocols and standards.

**In Summary:**

- The ISPS Code is meant for compliance regarding the provisions of Chapter XI-2 of the Annex to the International Convention for SOLAS.
- The ISPS Code is designed to improve security and better protect people and cargo, as well as ports and international shipping, against terrorism.
- The ship/port interface is seen as a potential point of weakness and liability for all current security measures.
- Sea perimeters are especially difficult to control and police.
- Other maritime security challenges external to the Code, are illegal immigration, smuggling, theft and piracy.
- The Code provides “identity” and “transparency”.

- It makes it clearer with whom business is being conducted and who is responsible for what.
- Currently, it is often unclear who is the beneficial owner of a vessel and who is responsible for its conduct.

There is very little time between now and 1 July 2004 for ships and port facilities to comply with the ISPS Code. Bodies such as Classification Societies and Owner Organizations are providing advice and guidance to their members, but total clarification is not yet available as to how the ISPS Code will be implemented and judged in actual practice.

It is unlikely that the implementation date of 1<sup>st</sup> July 2004 will be extended. In spite of this fact, some countries have yet to decide which national body is responsible for ship and port security and therefore, may not have appointed a “Recognized Security Organization” (RSO), which it left to individual companies (in this case, the shipping lines and security underwriters) as being the accepted bodies who will certify and issue the International Ship Security Certificate.

It has been stated by major organizations that ‘worldwide’ as many as 30,000 to 40,000 ships will require an International Ship Security Certificate (ISSC) from an independent and approved body. This process, which in itself will be quite a lucrative contract to whoever gets selected to do so, introduces an element of doubt in relation to the ability of some ships (and ports) to comply with the ISPS Code on time. Those above business groups (and some 15,000 to 20,000 ports in turn), will have to hire qualified experts to identify their individual ISPS Code security risks for them, as well as come up with a port or ship security plan (if the Port Authorities accept them) and these also need to be approved by their Contracting Governments.

An International Ship Security Certificate (ISSC) is either granted or it is not. Failure to gain an ISSC means that the said vessel cannot trade its cargo.

Every vessel subject to the ISPS Code should have a Ship Security Plan in place by April 2004.

The ISPS Code recognizes that threats to individual nations national security may come from a ship via its personnel, cargo or the ship itself. It also recognizes that in turn, a ship is also vulnerable to threats from terrorists, organized crime, port personnel, cargo and stores, and the port facility itself.

Good record maintenance and retrieval of security records and contacts between the ship and port facilities is an essential part of qualifying for an ISSC – International Ship Security Certificate.

One method of co-ordination that the ISPS Code aims to achieve between a ship and port facility after 1 July 2004 includes a “Declaration of Security” between the ship and port facility.

The Flag and Port States are responsible for ensuring that news and information on security affecting ships reaches affected vessels in a timely manner.

Flag, port and coastal states must know where ships are. This has implications for long-range identification and tracking of ships, although this is still being developed.

The IMO has still yet to decide on how Long Range Ships’ Identification and Tracking will operate. The issue will be discussed again at COMSAR 8 in February 2004, at MSC78 in June 2004 and MSC79 in December 2004.

Some national governments are applying the ISPS Code to their domestic ships and port facilities. Some national governments are introducing their own domestic maritime legislation.

Examples include the USA with the Maritime Transportation Security Act, 2002 and the European Commission’s May 2003 proposals for enhancing maritime transport security. Some international organizations, e.g. OECD on the ownership of ships/fleets, are considering new regulations for maritime transport. A EU directive on Port Security may materialize.

There are three designated levels of security under the ISPS Code:

Normal	(level 1)
Increased	(level 2)
High	(level 3).

At varying dates, every ship subject to the ISPS Code must install a Ship Security Alert System (SSAS). This is a covert alert, which does not sound on the ship nor will it alert neighbouring ships – it alerts the authorities ashore only.

The method of alert for the SSAS varies according to whether the equipment used to give the covert alert is GMDSS approved or not. Alerts that use GMDSS equipment will be sent to the Rescue Co-ordination Centre (RCC) or a designated national security authority. Alerts via Non-GMDSS equipment may be sent to any designated destination, e.g. service provider.

The International Labor Organization (ILO) has agreed to revise its regulations for seafarers’ ID in regards to background checks.

Further regulation on Port security, which is likely to be complimentary to the ISPS Code, is ‘rumoured’ to be in the offing from the European Commission. Further, IMO updates on the ISPS Code and related issues will appear when available.