

## Chapter 6

# SECURITY

Inland tankers and barges often load or unload at facilities where seagoing tankers are being handled and thus where the International Ship and Port Facility Security (ISPS) Code is applicable. This Chapter provides a brief summary of the major provisions of the International Ship and Port Facility Security (ISPS) Code.

In addition, Section 6.5 provides guidance on the content and structure of security plans for inland tankers.

### 6.1 General

International seagoing tankers, and terminals handling such tankers, are required to take measures to enhance marine security and to be in compliance with the provisions of the International Ship and Port Facility Security (ISPS) Code, Parts A & B. The Code is detailed in Chapter XI-2 of the International Convention for the Safety of Life at Sea (SOLAS).

Terminals should note that this is the first occasion on which the SOLAS Convention has been applied to shore-based facilities in states that are party to the Convention.

It is recommended that all seagoing tankers and terminals should have a security plan with procedures to address all security aspects identified from a security assessment. Tankers and terminals which are not required to comply with the SOLAS and ISPS Code are encouraged to consider the provisions of SOLAS and the ISPS Code when developing their security plans.

Legislation may require inland waterways tankers and terminals to apply specific security measures. It is recommended that when inland tanker barges visit terminals and facilities where the ISPS Code is mandatory, or where legislation regulates security measures, these measures harmonise with the requirements of the ISPS Code to avoid gaps in security.

### 6.2 Security Assessments

The security assessment for terminals and seagoing tankers should include a risk analysis of all aspects of the tanker's and terminal's operations in order to determine which parts of them are more susceptible and/or more likely to be the subject of a security incident. The risk is a function of the threat of a security incident, coupled with the vulnerability of the target and the consequences of the incident. The security assessment should, as a minimum, encompass the following items:

- Identification of existing security measures, procedures and operations in effect on board the tanker or at the terminal.

- Identification and evaluation of key assets and infrastructure it is important to protect.
- Perceived threats to the tanker or terminal facility and their likely occurrence.
- Potential vulnerabilities and consequences of potential incidents to tankers, terminals, berths and tankers at the berths.
- Identification of any weaknesses (including human factors) in the infrastructure, policies and procedures.

### 6.3 Responsibilities Under the ISPS Code

For a terminal, responsibility for the security plan rests with the terminal management and may, depending upon the circumstances at the terminal, require a designated security officer who has the necessary skills and training to ensure full implementation of the security measures at the terminal.

For a seagoing tanker, the Company's responsibility for the plan rests with the Company Security Officer. However, the Master has overriding authority to make decisions regarding the safety and security of the tanker. A designated Ship Security Officer should be appointed who has the necessary skills and training to ensure full implementation of the measures required to be in place on board the tanker. This function may be conducted by the Master, although often one of the senior officers will be appointed.

### 6.4 Security Plans

The security plan will vary from terminal to terminal and from seagoing tanker to seagoing tanker depending on the particular circumstances identified by the security assessment, requirements for compliance with SOLAS and the ISPS Code, and local and national security considerations. The plan should describe:

- The security organisation on board the seagoing tanker or at the terminal and port as appropriate.
- Basic security measures for normal operation and additional measures that will allow the seagoing tanker and terminal to progress, without delay, to increased or lowered security levels as the threat changes.
- Procedures for interfacing the security activities of seagoing tankers and terminals with those of local port authorities, other tankers, terminals and dock facilities in the region and other local authorities and agencies (e.g. police and coast guard).
- Provision for regular reviews of the plan and for amendments based upon experience or changing circumstances.
- Measures designed to prevent unauthorised access to the seagoing tanker and terminal and in particular, measures to restrict access to vulnerable areas of a terminal and to restrict access to tankers when moored at the terminal, including the identification of tanker and terminal personnel (such as by identity documents or identification badges).

- Measures designed to prevent unauthorised weapons, dangerous substances or devices intended for use against persons, tankers or terminals from being taken on board the tanker or from being introduced to the terminal.
- Procedures for responding to security threats or breaches of security, which may include evacuation.

For seagoing tankers, the ICS publication “Model Ship Security Plan” should be referred to. It can be adapted according to the security needs of individual tankers.

## 6.5 Security Plans for Inland Tankers

The security plan for inland tankers will vary from one inland tanker to another depending on the particular circumstances identified by the security assessment, requirements for national and/or international legislation, and local and national security considerations. The plan should describe and comprise at least the following elements:

- a) specific allocation of responsibilities for security to competent and qualified persons with appropriate authority to carry out their responsibilities;
- b) records of dangerous goods or types of dangerous goods concerned;
- c) review of current operations and assessment of security risks, including any stops necessary to the transport operation, the keeping of dangerous goods in the vessel, tank or container before, during and after the journey and the intermediate temporary storage of dangerous goods during the course of intermodal transfer or transshipment between units;
- d) clear statement of measures that are to be taken to reduce security risks, commensurate with the responsibilities and duties of the participant, including:
  - training;
  - security policies (e.g. response to higher threat conditions, new employee/employment verification, etc.);
  - operating practices (e.g. choice/use of routes where known, access to dangerous goods in intermediate temporary storage (as defined in (c)), proximity to vulnerable infrastructure etc.);
  - equipment and resources that are to be used to reduce risks;
- e) effective and up to date procedures for reporting and dealing with security threats, breaches of security or security incidents;
- f) procedures for the evaluation and testing of security plans and procedures for periodic review and update of the plans;
- g) measures to ensure the physical security of transport information contained in the security plan; and
- h) measures to ensure that the distribution of information relating to the transport operation contained in the security plan is limited to those who need to have it.

## 6.6 Declaration of Security (DoS)

Based on ISPS legislation, a Declaration of Security may be completed by the seagoing tanker and the inland tanker. The declaration describes detailed information about mutually agreed security measures taken. The following provides an example of the content of a DoS:

## Declaration of Security

between a ship and other ship which it interfaces with

Name of ship	Name of other ship
Port of registry	Port of registry
IMO Number.	IMO Number.

This Declaration of Security is valid from..... until .....  
for the following activities: .....  
..... under the following security levels

Security level(s) for the ship:

Security level(s) for the other ship:

The ship and the other ship agree to the following security measures and responsibilities (as applicable) to ensure compliance with the requirements of part A of the International Code for the Security of Ships and of Port facilities.

The affixing of the initials of the master or SSO under these columns indicates that the activity will be done, in accordance with the relevant approved plan, by

Activity	The ship :	The other ship :
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the ship		
Controlling access to the other ship		
Monitoring of the areas surrounding the ship.		
Monitoring of the areas surrounding the other ship		
Handling of cargo		
Delivery of ship's stores		
Handling of unaccompanied baggage		
Controlling the embarkation of persons and their effects.		
Ensuring that security communication is readily available between the ships		

The signatories to this agreement certify that security measures and arrangements for both ships during the specified activities meet the provisions of chapter XI-2 and part A of the Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex

Dated at .....on the .....

Signed for and on behalf of	
The ship :	The other ship :

(Signature of master or ship security officer)      (Signature of master or ship security officer)

Name and title of person who signed	
Name:	Name:
Title:	Title:

Contact details	
Master:	Master:
Ship security officer:	Ship security officer:
Company:	Company:
Company security officer:	Company security officer:
Telephone number:	Telephone number:
Radio Channels:	Radio Channels: