



**DNV Guideline  
to  
International Ship Security  
Certification**

**Det Norske Veritas – July 2007**

**Det Norske Veritas (DNV)** is an autonomous, independent foundation with the objective of safeguarding life, property and the environment. The DNV organization comprises 300 offices in 100 countries, with a total of 7000 employees.

#### **Liability and Indemnity**

If any person suffers loss or damage, which is proved to have been caused by any negligent act or omission of Det Norske Veritas, then Det Norske Veritas shall pay compensation to such person for his proved direct loss or damage. However, the compensation shall not exceed an amount equal to ten times the fee charged for the service in question, provided that the maximum compensation shall never exceed USD 2 million.

In this article "Det Norske Veritas" shall mean the Foundation Det Norske Veritas as well as its subsidiaries, directors, officers, employees, agents and any other acting on behalf of Det Norske Veritas.

# DNV Guideline to International Ship Security Certificate

## A smooth transition towards the Security regime

### Contents

<b>1</b>	<b>INTRODUCTION</b> .....	<b>4</b>
1.1	BACKGROUND .....	4
1.2	DNV'S ROLE .....	4
<b>2</b>	<b>SOLAS AND THE ISPS CODE</b> .....	<b>4</b>
2.1	OVERVIEW .....	4
2.2	IMO REQUIREMENTS TO THE SHIP SECURITY ASSESSMENT .....	5
2.3	IMO REQUIREMENTS TO THE SHIP SECURITY PLAN.....	6
2.4	OTHER SOLAS AND ISPS CODE REQUIREMENTS .....	6
2.5	DEFINITIONS FROM SOLAS AND THE ISPS CODE .....	6
<b>3</b>	<b>SECURITY CERTIFICATION PROCESS</b> .....	<b>9</b>
3.1	GENERAL.....	9
3.2	REQUIRED INDEPENDENCE .....	9
3.3	SCOPE OF CERTIFICATION .....	9
3.4	COMPANY REQUEST .....	9
3.5	SHIP SECURITY ASSESSMENT (SSA).....	9
3.6	SHIP SECURITY PLAN (SSP) .....	9
3.7	SHIPBOARD VERIFICATION OF IMPLEMENTATION OF THE SSP.....	10
3.8	INTERNATIONAL SHIP SECURITY CERTIFICATE (ISSC).....	10
3.9	INTERIM CERTIFICATION .....	10
<b>4</b>	<b>DNV RECOMMENDATIONS AND INTERPRETATIONS</b> .....	<b>11</b>
4.1	SHIP SECURITY PLAN .....	11
4.2	SHIPBOARD VERIFICATION .....	11
4.3	SECURITY EQUIPMENT .....	12
4.4	COMMUNICATION OF INFORMATION .....	12
4.5	MISCELLANEOUS.....	12
<b>5</b>	<b>DNV AUTHORISATIONS</b> .....	<b>12</b>
<b>6</b>	<b>TRAINING AND OTHER ASSISTANCE</b> .....	<b>12</b>
6.1	COMPETENCE REQUIREMENTS .....	12
6.2	DNV SEASKILL™.....	12
6.3	CONSULTING AND ADVISORY SERVICES .....	13
<b>7</b>	<b>GUIDELINES FOR PERFORMING SHIP SECURITY ASSESSMENTS AND SHIP SECURITY PLANS</b> .....	<b>13</b>
<b>8</b>	<b>ADDITIONAL INFORMATION AND REFERENCES</b> .....	<b>13</b>
<b>9</b>	<b>CHECKLIST FOR SHIP SECURITY PLAN</b> .....	<b>14</b>

# 1 Introduction

## 1.1 Background

The following describes an overview of the process on how DNV can assist a ship-owner or manager to acquire the International Ship Security Certificate (ISSC).

The ISSC is required for the following ships in international trade:

- all passenger ships including high-speed passenger craft
- cargo ships above 500 GT
- mobile offshore drilling units

The certificate is issued in accordance with SOLAS chapter XI-2 and the International Ship and Port Facility Security (ISPS) Code adopted by IMO in December 2002. The Code has been in force since 1 July 2004.

Shipping Companies are required to perform a Ship Security Assessment (SSA) for each ship in the fleet. Based on this assessment, a Ship Security Plan (SSP) for each ship in the fleet will be developed. SOLAS and the ISPS Code also set a number of requirements to Companies and their security organisation, but these are not subject to certification. However, findings onboard a ship may result in activities/actions within the Company.

## 1.2 DNV's role

DNV is authorised by more than 50 Flag States as a Recognised Security Organisation (RSO). As an RSO, DNV is normally delegated the responsibility to review and approve Ship Security Plans, to verify that the plans are implemented onboard and to issue the International Ship Security Certificate on behalf of the Flag State Administration. Authorisation scope may vary (e.g. some Flag Administrations are doing SSP approval and/or issuance of Full Term ISSC themselves).

ISPS verification is done by close to 200 DNV surveyors distributed around the world.

# 2 SOLAS and the ISPS Code

## 2.1 Overview

Ship owners and managers of ships have the responsibility for ensuring the security and safety of the ships under their operation. The security measures are centred on SOLAS ch. XI-2 and the ISPS Code. Part A of the ISPS Code is mandatory through amendments to SOLAS, Ch. XI-2. Part B of the ISPS Code has been drafted as guidance and is recommendatory. Relevant requirements in this part of the code are regarded as mandatory by several Flag Administrations (e.g. US and EU). Thus Part B is considered, also by DNV, to be mandatory, to ensure that ships having ISPS with DNV shall fulfil the requirements stated by all Contracting Governments.

In addition to all ships in international trade, the ISPS Code applies to port facilities serving ships engaged on international voyages.

An important aspect of the ISPS Code is the way security risk is treated. The vulnerability of ships and port facilities can be established independently, but the threat to ships and ports varies depending on external factors. Contracting Governments (Flag- Port- and Coastal States) shall therefore determine and set the appropriate security level for sea areas, coastal areas and ports based on intelligence information:

- Security Level 1: normal, minimum appropriate protective security measures shall be maintained at all times.
- Security Level 2: heightened, appropriate protective security measures shall be maintained for a period of time as result of heightened risk for a security incident.
- Security Level 3: exceptional, further specific protective security measures shall be maintained for a period of time when a security incident is probable or imminent.

It is the Contracting Government's responsibility to set the appropriate security level, and this responsibility cannot be delegated to an RSO or any other relevant body.

The current security level creates a link between the ship and the port facility, since it triggers implementation of appropriate security measures for both parties. The Code requires a methodology for security assessments to be made, and plans and procedures to react to changing security levels shall be established, based on the SSA.

The Ship Security Plan (SSP) shall address the appropriate measures for the ship (and port) to move from security level 1 to 2, and from 2 to 3.

All Companies operating ships have to designate and provide training for a Company Security Officer (CSO), and, for each ship, a Ship Security Officer (SSO). Some Flag Administrations also require appointed deputies for these positions.

## **2.2 IMO requirements to the Ship Security Assessment (SSA)**

Part A, section 8 of the ISPS Code stipulates that the SSA is to include an on-scene security survey and, at least, the following elements:

- identification of existing security measures, procedures and operations
- identification and evaluation of key ship board operations which is important to protect
- identification of possible threats to the key ship board operations and the likelihood of their occurrence, in order to establish and prioritise security measures
- identification of weaknesses, including human factors in the infrastructure, policies and procedures.

Prior to commencing the SSA, the Company Security Officer (CSO) shall ensure that advantage is taken of information available on threat assessment for the voyage pattern and the ports at which the ship is calling. For ships trading between two (or more) fixed ports, these ports should be taken into account in the SSA. For ships on the spot market, however, ports of call may be difficult to envisage, and for such situations the Company must decide which voyage pattern and ports it wants to use in the SSA (and the related SSP).

The CSO is also to ensure that the assessment is carried out by persons with appropriate skills to evaluate the security of the ship. Importantly, the SSA is to be documented, reviewed, accepted and retained by the Company.

Part B, section 8 of the ISPS Code gives further guidance to how an SSA shall be carried out, and reference to other guidelines is given in section 7 of this document.

## 2.3 IMO requirements to the Ship Security Plan (SSP)

According to the ISPS Code Part A, the SSP shall be developed based on the SSA, and shall, among other items, address measures to prevent access of unauthorised persons and to prevent carriage of unauthorised cargo, stores or other items.

Procedures for training, drills, audits, reporting of security incidents, periodic review of the SSP and interface with port facilities shall be addressed. The SSP is to address response to security threats and response to security instructions from Authorities.

The SSP shall also identify restricted areas onboard and measures to prevent unauthorised access to them. Procedures for monitoring the security of the ship are to be implemented.

## 2.4 Other SOLAS and ISPS Code requirements

An important requirement in the ISPS code is the provision of security records. Records of all security activities shall be kept onboard and these records may be subject to Port State Control. In general, Port State Control will verify that the ship carries a valid Ship Security Certificate, and unless there are specific "clear grounds", the Port States do not have general access to the Ship Security Plan. Inspection of the records is an important additional means for the Port State to establish that the ship is in compliance with the ISPS Code.

The Ship is required to keep onboard information on who is responsible for appointing the crew and deciding the employment of the Ship. This may also be subject to inspection by Port States.

SOLAS requires that all ships shall be provided with a Ship Security Alert System (SSAS) which, when activated, initiates and transmits a ship-to-shore security alert to a competent authority designated by the Administration.

## 2.5 Definitions from SOLAS and the ISPS Code

**"Ship/port interface"** means the interactions which occur when a ship is directly and immediately affected by actions involving the movement of people, goods or the provisions of port services to or from the ship.

**"Ship-to-ship activity"** means any activity not related to a port facility that involves the transfer of goods or persons from one ship to another.

**"Security incident"** means any suspicious act or circumstance threatening the security of the ship, including a mobile offshore drilling unit and a high-speed craft, or of a port facility or of any ship/port interface or any ship-to-ship activity.

**"Declaration of Security" (DoS)** means an agreement reached between a ship and either a port facility or another ship with which it interfaces, specifying the security measures each will implement.

**"Recognized Security Organization" (RSO)** means an organization with appropriate expertise in security matters and with appropriate knowledge of ship and port operations authorized to carry out an assessment, or a verification, or an approval or a certification activity, required by SOLAS or by part A of the ISPS Code.

**"Ship Security Plan" (SSP)** means a plan developed 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.

**"Port Facility Security Plan" (PFSP)** means a plan developed 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.

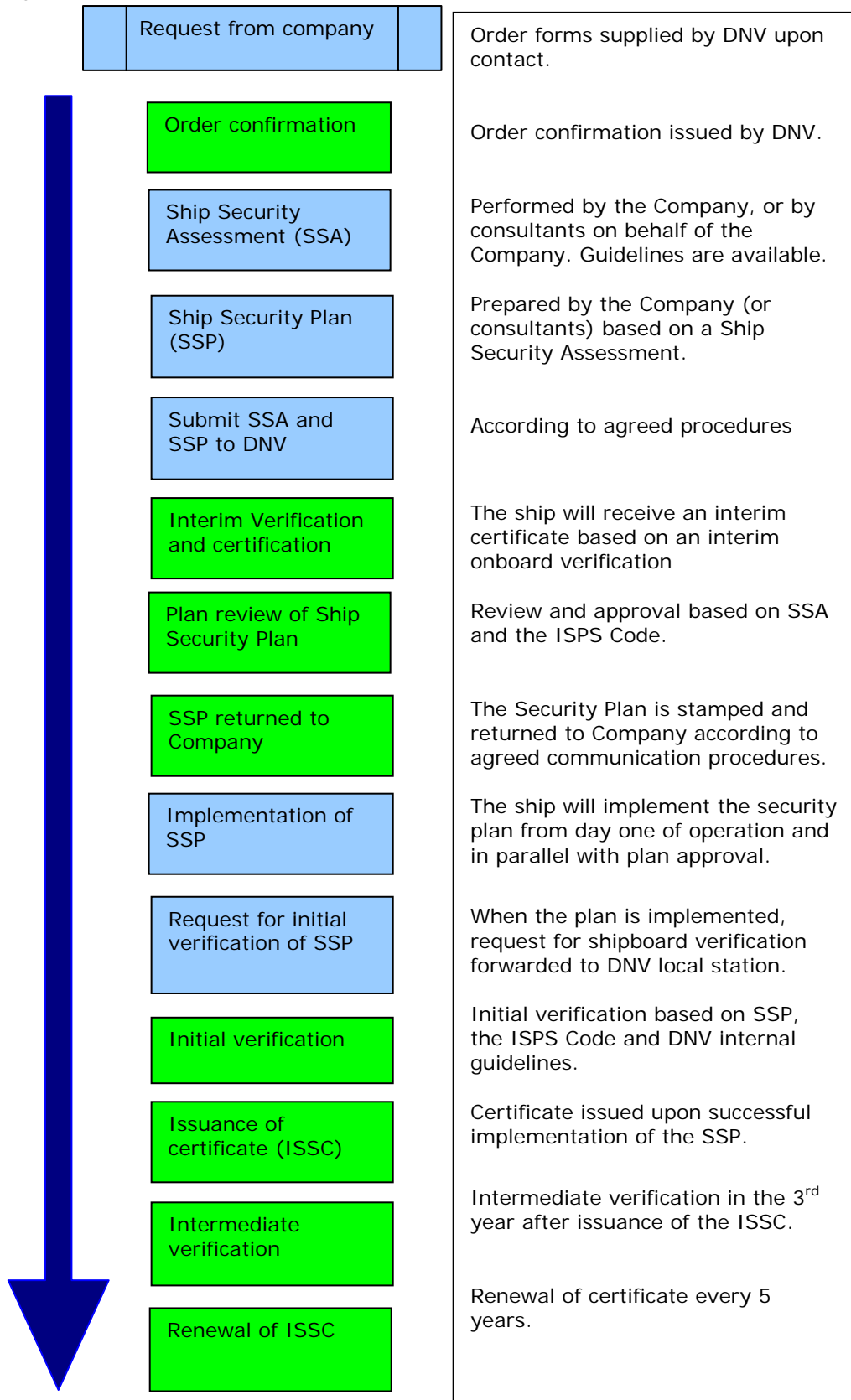
**“Ship Security Officer” (SSO)** means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan, and for liaison with the company security officer and port facility security officers.

**“Company Security Officer” (CSO)** means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained, and for liaison with Port Facility Security Officers and the Ship Security Officer.

**“Port Facility Security Officer” (PFSO)** means the person designated as responsible for the development, implementation, revision and maintenance of the Port Facility Security Plan and for liaison with the Ship Security Officers and Company Security Officers.

## Certification Process Flowchart

Company  
 DNV



## **3 Security Certification Process**

### **3.1 General**

The International Ship Security Certificate is issued following a successful verification of the implemented Security System.

The ISPS Code gives requirements to the Company and the Ship. These requirements are partly functional as set down in SOLAS ch. XI-2 and the ISPS Code part A, and partly prescriptive requirements outlined in Part B of the Code. The specific security measures are to be determined through the SSA and by procedures documented in the SSP. The implementation of the SSP is to be verified in an Initial Shipboard Verification.

The certification process is to verify that all requirements of SOLAS chapter XI-2 and the ISPS Code are met. The process is illustrated in the flowchart above and the steps of the process are explained in more detail in the following. The introduction to Part B of the ISPS Code gives an overall view of the security regime within the shipping industry.

### **3.2 Required independence**

DNV cannot engage in the development of an SSP, and later approve the same plan. This is clearly stated in the ISPS Code. However, DNV will respond to general questions regarding SOLAS and the ISPS Code, and provide DNV's understanding and interpretations of regulations.

### **3.3 Scope of Certification**

SOLAS XI-2/3.3 states that the Company shall comply with the relevant requirements of SOLAS XI-2 and of part A of the ISPS Code, taking into account the guidance given in Part B of the ISPS Code. DNV considers relevant requirements in Part B to be mandatory, and this shall be stated in the SSP. Flag state interpretation and specific requirements vary and must be adhered to. The Company itself is not subject to certification, but an efficient implementation of the security system onboard relies on the Company's active participation in the process.

### **3.4 Company request**

DNV will supply an order form for security certification. The information required is necessary to plan the process in the most efficient way. A contract will be signed between DNV and the Company for the scope of work, and as the SSA and parts of the SSP are regarded as confidential, procedures for communication of such information between DNV and the Company will be settled at this stage.

### **3.5 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 (SSP). The Company Security Officer shall ensure that an SSA is carried out for each ship in the fleet. The CSO needs not necessarily personally undertake all the duties associated with performing the SSA. The SSA is to be carried out by persons with appropriate skills, and the Company may consult experts or consultants as found necessary. The SSA shall, however, be documented, reviewed, accepted and retained by the Company.

The SSA is not subject to approval, but an evaluation of the assessment will be carried out during the SSP review and approval. DNV will base this evaluation on the formal requirements given in the ISPS Code Part B, section 8.

### **3.6 Ship Security Plan (SSP)**

The Company Security Officer is responsible for the development of a Ship Security Plan for each ship.

It is important that all risks identified in the SSA are addressed in the SSP. Requirements in SOLAS Ch. XI-2 and the ISPS code part A as well must be complied with. In addition all relevant requirements given in Part B of the ISPS are considered by DNV to be mandatory for the purpose of ship security certification. The reason for this is that major port states have stated that Part B should be considered mandatory, and will expect documentation to that effect.

It is considered important that the SSP, when describing security measures, allows for redundancy in the security procedures, especially with regards to technical equipment. Failure of a piece of equipment should not lead to a non-conformity with the security system and hence non-compliance with the ISPS code, but should rather be handled by contingency plans.

The Company should establish procedures to restrict the distribution, disclosure, and availability of information contained in the SSP. Access to the SSP should be restricted to those persons with an operational need to know. A copy of the SSP will be kept onboard the ship in a secure location, and shall be made available to the DNV Security Surveyor.

When the plan is forwarded to DNV for approval, DNV will review and approve the SSP based on the SSA and the requirements of SOLAS and the ISPS Code. Submission of an SSP must be accompanied by the SSA on which it is based. The plan will be stamped, sealed and returned to the Company. If non-conformities are identified, the plan will be returned to the Company with comments. In case DNV is not authorised by the Flag Administration to approve the SSP, the approval is normally done by the Flag. If DNV is still asked to review the SSP, a Statement of Compliance may be issued, but the plan cannot be stamped and signed as approved by DNV.

### **3.7 Shipboard Verification of implementation of the SSP**

When the Company considers the plan to be properly implemented on board the ship, a request for verification should be sent to the DNV Customer Service Manager. An onboard verification will then be arranged at a convenient time and place. The onboard verification is expected to take 1-2 days depending on the ship type and complexity.

### **3.8 International Ship Security Certificate (ISSC)**

The ISSC will be issued upon a complete verification of the ship's security system when the ship is found to fully comply with SOLAS and the ISPS Code. The ISSC is valid for 5 years subject to intermediate verification between the 2<sup>nd</sup> and 3<sup>rd</sup> anniversary. For Flag States where DNV is not authorised to issue the full term ISSC, DNV will normally have authorisation to issue a short term ISSC. Copy of the verification report and short term ISSC will be forwarded to the Flag State Authorities to initiate the issuance of the full term certificate.

### **3.9 Interim Certification**

For a new ship, or for an existing ship where the ISPS responsible manager or Flag has changed, the ISPS Code permits issuance of an interim ISSC for a period of up to 6 months, pending approval of the new SSP and initial verification onboard. Note, however, that prior to issuance of the interim ISSC, the SSA and the SSP must have been completed, provided onboard for implementation and forwarded to DNV for approval.

During the interim period of up to 6 months, relevant records shall be built up, but even if the effectiveness of the implemented system will be improved during this period, the system shall be sufficiently implemented onboard to ensure a "secure ship" from day one.

### **3.10 Handling of change scenarios**

Required verification/certification actions by DNV when the ship's conditions are changed are as follows:

<b>Change Scenario</b>	<b>Case conditions</b>	<b>Verification/certification actions</b>
Change of ship's name		Replacement ISSC is issued
Change of flag	DNV has not done shipboard verification under the previous flag	Full initial verification is done and ISSC with 5 years validity is issued.
	DNV has done shipboard verification under the previous flag	Additional verification is done and a new ISSC is issued with the same expiry date as the previous ISSC.
Change of manager		Interim verification is done and interim ISSC is issued.
Change of company name and/or address		Replacement ISSC is issued with the same expiry date as the previous ISSC.

In addition some SSP approval activities may be required.

## **4 DNV Recommendations and Interpretations**

### **4.1 Ship Security Plan**

To be able to make an accurate and speedy approval of an SSP, DNV recommends that all relevant ship data are listed in the plan (ship type, trade, cargo, size parameters, etc.) and that a general arrangement with restricted areas identified accompanies the plan. Access points and shell doors should also be identified on the drawing.

The SSA should include a set of conditions, such as area of trade and cargoes carried, which the assessment is based upon. It follows that the SSA may not be valid if these conditions change significantly.

Likewise, the SSP should include the same set of criteria which were used for the SSA.

It is also recommended to include a tabular listing of all ship related ISPS Code requirements with cross reference to where in the SSP the issue is covered. If a requirement is not relevant or not fulfilled for the ship, the reason should be documented in the table. See also section 9 of this document.

The plan should give clear instructions on who has access to the plan and, if applicable, on who's authority.

The SSP should state clear objectives in accordance with the Company Security principles, and outline a policy on how to achieve these objectives.

It is recommended that procedures for keeping records are established and stated in the SSP.

### **4.2 Shipboard Verification**

The ISPS Code requires that the ship undertakes an internal audit of the security system onboard, and duly notes this in the security records prior to the initial shipboard verification. The internal audit should be performed by persons independent of the activities being audited.

At least one security drill should be performed and documented in the Security Records during the implementation period. A security drill may also be requested as part of the shipboard verification.

### **4.3 Security equipment**

Security equipment is equipment described in the SSP as having a specific security function onboard. All security equipment is required to be maintained, inspected, tested and calibrated and the SSP shall contain procedures for such, including frequency for testing and calibration. Verification of equipment is limited to a functional test according to stated procedures and recommended practice.

The Ship Security Alert System (SSAS) is part of the security equipment on board and the system is required for all ships. Procedures, instructions and guidance on use of the SSAS, including testing, activation, deactivation, resetting and actions to limit false alerts shall be contained in the SSP, either directly or by cross reference to other documents.

The SSAS shall be type approved or case approved by the Flag State.

### **4.4 Communication of information**

The Ships and Companies are required to have information of names and contact details of Flag States and Port State Authorities responsible for Security Issues, including Port Facility Security contacts. This information is made available to IMO by the Authorities for posting in the IMO GISIS database.

### **4.5 Miscellaneous**

Some items referred to in SOLAS Chapter XI-1, Ship Identification Number and Continuous Synopsis Record, are not part of the scope for Security Certification and will be dealt with through the Safety Certification regime. The Automatic Identification System required by SOLAS chapter V is likewise not part of the Security Certification, but covered through the Safety Equipment regime.

Provisions have been made within the regulatory system in IMO for future amendments to the security regulations to be brought into force in the shortest possible time.

## **5 DNV Authorisations**

DNV are authorised by most major Flag States to act as an RSO on their behalf. Some Flag States do however not delegate this responsibility outside their own administration and some have given a partial authorisation. Please contact the DNV Customer Service Manager at the DNV Station closest to you for information.

## **6 Training and other Assistance**

### **6.1 Competence requirements**

No formal competence requirements for the position as Ship Security Officer or Company Security Officer are yet implemented in the STCW Convention; however, IMO has prepared a model course for Company and Ship Security Officers. Documentation that the SSO has been given training must be found onboard. Unless specifically required by the Flag Administration, such training must not be through an approved course, but may be company internal training.

### **6.2 DNV SeaSkill™**

DNV SeaSkill™ is a unit of DNV, certifying and coordinating training programmes to the Maritime Industry. This includes training for Maritime Security.

The actual training will mainly be provided by established Maritime Security consultants, which have been screened and certified by DNV. Such training courses include:

- Company Senior Managers Training (one day course)

- Company Security Officers Training (3-5 day course)
- Ship Security Officers Training (3-5 day course)
- Shipboard Personnel Security Awareness Training (variable duration)

Some of the basic training will be provided through computer based training (CBT), or video.

DNV SeaSkill™ will certify the training programs to verify that they meet the requirements of the ISPS Code, and the IMO Model Course.

For additional information on DNV SeaSkill™, please contact:

DNV SeaSkill™

Det Norske Veritas

1322 Høvik

Telephone +47 67 57 91 65 / 94 76 / 83 01

Email: [seaskill@dnv.com](mailto:seaskill@dnv.com)

Web: <http://www.dnv.com/Maritime/SeaSkill/>

or any DNV Station.

### 6.3 Consulting and Advisory Services

To avoid possible conflicts of interest, DNV will not be involved in security consulting and advisory services. However, DNV has prepared a separate list of companies that can offer services within this area, for instance related to assistance with development of ships security assessments and ship security plans. Some of these companies also offer security training certified by DNV SeaSkill™.

Please contact any DNV Station for further information.

## 7 Guidelines for performing Ship Security Assessments and Ship Security Plans

Additional information for performing SSAs and preparing SSPs may be found in the Norwegian Shipowners' Association (NSA) Guidelines for performing SSA that is available from the non-public part of the NSA website: <http://www.rederi.no/en/> and US Coast Guard NVIC 10-02 is available at: <http://www.uscg.mil/hq/g-m/nvic/index.htm>

## 8 Additional Information and References

International Maritime Organisation [www.imo.org](http://www.imo.org)

International Chamber of Commerce weekly piracy report [www.iccwbo.org](http://www.iccwbo.org)

Maritime Security Council [www.maritimesecurity.org](http://www.maritimesecurity.org)

The U.S. Office of Naval Intelligence [http://164.214.12.145/onit/onit\\_j\\_main.html](http://164.214.12.145/onit/onit_j_main.html)

European Association of Airport and Seaport Police [www.eaasp.org](http://www.eaasp.org)

US Dept of State Counter-Terrorism Office [www.state.gov](http://www.state.gov)

Overseas Security Advisory Council [www.osac.gov/](http://www.osac.gov/)

Central Intelligence Agency [www.cia.gov](http://www.cia.gov)

Interpol [www.interpol.int](http://www.interpol.int)

Federal Bureau of Investigation [www.fbi.gov](http://www.fbi.gov)

The Terrorism Research Centre [www.terrorism.com](http://www.terrorism.com)

## 9 Checklist for Ship Security Plan

This checklist is developed for the Company to assess the status of their Ship Security Plan and Ship Security Assessment. It is intended for the Company to check that major items are covered, and to decide when the plan is ready to be submitted to DNV for approval.

This checklist is not intended to be used as a detailed guide for development of SSP, and does not give a complete overview of the ISPS Code contents and requirements, but it does give an overall structure of an SSP. Reference to "DNV", means that the item is a DNV requirement. Special Flag state requirements may apply.

DNV report reference	ISPS Code reference	SOLAS XI-2 and ISPS Code Requirements	Yes /No
<b>1</b>		<b>GENERAL</b>	
1.1	DNV	<b>Introduction</b> Company objective and policy	
1.2	DNV	<b>Ship, port and trade specific data</b> ports that the ship is likely to enter	
1.3	DNV	<b>Ship data</b> General arrangement with restricted areas, shell doors, ship type, size parameters, trade, cargo, etc	
1.4	DNV	<b>Scope and limitations</b> The SSP should include a set of conditions, like area of trading and cargo carried, and note that the SSA may not be valid if conditions change significantly	
1.5	DNV	<b>Restricted distribution</b> instructions as to who has access to the plan	
<b>2</b>	ISPS A 9.3 ISPS B 9.3	<b>SECURITY ASSESSMENT</b> A ship security assessment must be performed	
	DNV	The SSA should include a set of conditions, like area of trading and cargo carried, and it should be noted that the SSA may not be valid if conditions change significantly.	
2.1	ISPS A 8.5	<b>General</b> The ship security assessment shall be documented, reviewed, accepted and retained by the Company.	
2.2	ISPS A 8.2 ISPS B 8.13	<b>Qualifications</b> The ship security assessment is carried out by competent persons with skills to evaluate the security of a ship.	
2.3	ISPS B 8.4	<b>Expert assistance</b> Those involved in an SSA should be able to draw on expert assistance	
2.4	ISPS B 8.2 ISPS B 8.5	<b>Information required</b> Information available on the assessment of threat for the ports	
2.5	ISPS B 8.3	<b>Elements to include as part of the assessment</b> Identify security issues onboard	
2.6	ISPS A 8.4 ISPS B 8.8	<b>Protection</b> Identification of key shipboard operations	
2.7	ISPS B 8.6	<b>Examination of access</b> Identify points of access	
2.8	ISPS A 8.4.1 ISPS B 8.7-8	<b>Existing measures</b> Relevance of the existing security measures	
2.9	ISPS A 8.4.3 ISPS B 8.9	<b>Possible threats</b> Identification of possible threats	
2.10	ISPS A 8.4.4 ISPS B 8.10-12	<b>Potential vulnerabilities</b> Take into account all possible vulnerabilities	
2.11	ISPS A 8.4 ISPS B 8.14	<b>On-scene security survey</b> On-scene security survey has been carried out	
<b>3</b>		<b>SHIP SECURITY PLAN - DOCUMENTATION</b>	
3.1	ISPS A 9.4	<b>General</b> SSP shall be written in the working language of the ship.	
3.2	ISPS A 6.1 SOLAS II-2/8	<b>Company statement</b> Clear statement emphasizing the master's authority	
3.3	ISPS B 9.2, 9.7 ISPS A 7.2.7	<b>Ship organisation and communication</b> Detail of the organisational structure of the security of the ship and communication system	
3.4	ISPS A 9.4.14	<b>Company security officer (CSO)</b> Identification of the CSO	
3.5	ISPS A 12, 9.4.13	<b>Ship security officer (SSO)</b> Identification and duties of SSO	
3.6	ISPS A 13.2 ISPS B 13.1	<b>Qualifications of the SSO</b> The SSO shall have received training	
3.7	ISPS A 9.4.7 ISPS B 9.7.1	<b>Shipboard personnel</b> Duties of personnel with respect to security responsibilities	

DNV report reference	ISPS Code reference	SOLAS XI-2 and ISPS Code Requirements	Yes /No
3.8	ISPS A 13.3	<b>Shipboard personnel qualifications</b> (recommended)	
3.9	ISPS B 13.4	<b>Other shipboard personnel qualifications</b> (recommended)	
3.10	ISPS A 9.4.9 ISPS B 13.4-7	<b>Training, drills and exercises</b> procedures for training, drills and exercises	
3.11	ISPS A 9.4.8 ISPS B 9.53	<b>Audits</b> Procedures for auditing the security activities	
3.12	ISPS A 9.4.11	<b>Periodic review</b> Procedures for the periodic review of the SSP	
3.13	ISPS A 9.4.12 ISPS B 9.2.7 ISPS B.7.6	<b>Reporting</b> Procedures for reporting security incidents to the appropriate Contracting Governments contact points	
3.14	ISPS A 9.4.10	<b>Interface with port facilities</b> Interface with port facility security activities	
3.15	ISPS B 9.7.7	<b>Dangerous goods</b> Procedures for dangerous goods	
3.16	ISPS A 5.7 ISPS B 9.52	<b>Declaration of Security (DoS)</b> Procedures for handling of DoS	
3.17	ISPS A 9.6-8 ISPS B 9.7.4	<b>Administration of SSP</b> procedures to protect security sensitive information	
3.18	ISPS A 9.4.15 ISPS B 9.7.5	<b>Security equipment</b> type and maintenance requirements of security and surveillance equipment and systems	
3.19	ISPS A 9.4.17,18 SOLAS II-2/6	<b>Ship security alert system</b> Implementation date varies with ship types	
3.20	ISPS A 10	<b>Records</b> Procedures for keeping records	
3.21	SOLAS XI-2/5	<b>Crewing and charterers</b> (recommended) information to be kept onboard	
4	ISPS A 7 ISPS A 9.1 ISPS B 9.2.4,-5	<b>SHIP SECURITY MEASURES</b> Provisions for three security levels and procedures on how to escalate security measures from one level to the next	
4.1	ISPS A 7.2.2 ISPS A 9.4.3	<b>Access to the ship - general</b> Procedures for controlling access to the ship	
4.1.1	ISPS B 9.14	<b>Access to the ship - Security level 1</b>	
4.1.2	ISPS B 9.16	<b>Access to the ship - Security level 2</b>	
4.1.3	ISPS B 9.17	<b>Access to the ship - Security level 3</b>	
4.2	ISPS A 9.4.2 ISPS B 9.18-21	<b>Restricted areas</b> – general identification of restricted areas and measures for the prevention of unauthorized access	
4.2.1	ISPS B 9.22	<b>Restricted areas - Security level 1</b>	
4.2.2	ISPS B 9.23	<b>Restricted areas - Security level 2</b>	
4.2.3	ISPS B 9.24	<b>Restricted areas - Security level 3</b>	
4.3	ISPS A 7.2.6 ISPS B 9.25-26	<b>Handling of cargo</b> - general supervising the handling of cargo	
4.3.1	ISPS B 9.27-29	<b>Handling of cargo - Security level 1</b>	
4.3.2	ISPS B 9.30-31	<b>Handling of cargo - Security level 2</b>	
4.3.3	ISPS B 9.32	<b>Handling of cargo - Security level 3</b>	
4.4	ISPS A 7.2.6 ISPS B 9.33-34	<b>Delivery of ship's stores</b> - general	
4.4.1	ISPS B 9.35	<b>Delivery of ship's stores - Security level 1</b>	
4.4.2	ISPS B 9.36	<b>Delivery of ship's stores - Security level 2</b>	
4.4.3	ISPS B 9.37	<b>Delivery of ship's stores - Security level 3</b>	
4.5	ISPS B 9.38	<b>Handling of unaccompanied baggage</b> - general	
4.5.1	ISPS B 9.39	<b>Handling of unaccompanied baggage - Security level 1</b>	
4.5.2	ISPS B 9.40	<b>Handling of unaccompanied baggage - Security level 2</b>	
4.5.3	ISPS B 9.41	<b>Handling of unaccompanied baggage - Security level 3</b>	
4.6	ISPS A 7.2.5 ISPS B 9.42-44	<b>Monitoring the security of the ship</b> - general	
4.6.1	ISPS B 9.45-46	<b>Monitoring the security of the ship - Security level 1</b>	
4.6.2	ISPS B 9.47-48	<b>Monitoring the security of the ship - Security level 2</b>	
4.6.3	ISPS B 9.49	<b>Monitoring the security of the ship - Security level 3</b>	
4.7	ISPS B 9.50 ISPS A 7.7	<b>Differing security levels</b> establish procedures	
4.8	ISPS B 9.51	<b>Activities not covered by the code</b> establish procedures	
4.9	ISPS A 9.4.4	<b>Response to security threats</b> Procedures for responding to security threats	
4.10	ISPS A 9.4.5	<b>Response to security instructions</b> Procedures for responding to any security instructions	
4.11	ISPS A 9.4.6	<b>Evacuation</b> Procedures for evacuation in case of security threats	