Human Environment and Transport Inspectorate
Ministry of Infrastructure and Water Management

ItoS – SOLAS Chapter XI-2 - Maritime Security (ISPS)

Versie 2

Geldend vanaf: 09-06-2026 tot en met [nog niet bekend].

Documentgegevens

Dit document is een afdruk van een originele publicatie op PUC Open Data.

Originele versie:
Citeertitel: ItoS – SOLAS Chapter XI-2 - Maritime Security (ISPS)
Permalink: https://puc.overheid.nl/doc/PUC_802600_14

Soort document:
Type: Informatie voor uitvoering - Nieuwsbrief
Bron: Inspectie Leefomgeving en Transport

Versie en datums:
Versie: 2
Geldend vanaf: 09-06-2026 tot en met [nog niet bekend]
Laatste wijziging: 09-06-2026

Publicatiegegevens:
Uitgever: Inspectie Leefomgeving en Transport
Kanaal: ILT
Vorm: origineel PUC document
Referentienummer: PUC_802600_14
Toegankelijkheid: Extern
Publicatiedatum: 09-06-2026
Taal: en

Verrijking gepubliceerd bij document:
Thema: SOLAS Convention - Decisions and Interpretations
Hoofdtaak: Koopvaardij / Merchant Shipping

Inhoudsopgave

ItoS – SOLAS Chapter XI-2 - Maritime Security (ISPS)

Legend / Explanation of abbreviations:

- AIS: Automatic Identification System
- ASA: Alternative Security Agreement
- CSO: Company Security Officer
- CSR: Continuous Synopsis Record
- DA: Designated Authority
- DCC: Departmental Crisis Coordination Centre
- DGLM: Directoraat Generaal Luchtvaart en Maritiem
- DoS: Declaration of Security
- EU: European Union
- ESA: Equivalent Security Arrangement
- GMDSS: Global Maritime Distress and Safety System
- GISIS:Global Integrated Shipping Information System
- GT: Gross register Tonnage
- IACS: International Association of Classification Societies Ltd
- IEC: International Electrotechnical Commission
- ILT: Human Environment and Transport Inspectorate
- ILO: International Labour Organization
- IMO: International Maritime Organization
- ITC'69: International Convention on Tonnage Measurement of Ships 1969
- ISPS: International Ship & Port Facility Security Code
- ISSC: International Ship Security Certificate
- ITU: International Telecommunication Union
- KVNR: Royal Association of Netherlands Shipowners
- KWC:Netherlands Coastguard Centre Den Helder
- MSC: Maritime Safety Committee (IMO)
- NSI: Netherlands Shipping Inspectorate
- PFSO: Port Facility Security Officer
- PFSP: Port Facility Security Plan
- PI: Particular information
- PSO: Port Security Officer
- PSC: Port State Control
- RSO: Recognized Security Organization
- SOLAS: IMO Convention for the Safety of Life at Sea 1974
- SSA: Ship Security Assessment
- SSAS: Ship Security Alert System

- SSO: Ship Security Officer
- SSP: Ship Security Plan
- SSPI:Ship Security Pre-Arrival Information
- STCW: Standards of Training, Certification and Watchkeeping

1 General

1.1 Introduction

The IMO and EU have developed measures for the security of ships and port facilities. To improve the security of ships and port facilities, the (inter)national organizations has several instruments in place, such as Chapter XI-2 (special measures to enhance maritime security) of the SOLAS Convention and the ISPS Code which applies to all passenger ships, cargo ships with gross tonnage of 500 tons or more (engaged on international voyages), mobile offshore drilling units, and port facilities serving such ships engaged in international voyages.

This information is for the application of maritime security legislation (and interpretations) by ships flying the flag of the Netherlands.

1.2 General contact information

For the national contact point for direct security concerns, also in case of other ships (reference is made to SOLAS regulation XI-2/7.2), please contact the KWC.

Find the contactdetails for general (ship) security information on the website of the ILT.

2 Regulatory framework

The regulatory framework consists of:

- SOLAS Chapter XI-2 and the ISPS Code;
- Regulation (EC) No. 725/2004 on enhancing ship and port facility security;
- Policy Rule Safety Seagoing Vessels | Art. 2 Ship security;
- Regulation Safety Seagoing Vessels (Dutch);
- IACS Procedural Requirements No.24 | ISPS Code Certification (as revised); and
- ItoR(S)O no. 25 – SOLAS Chapter XI-2 - Maritime Security (ISPS).

Please note that there are, besides this ItoS – Security (ISPS), further instructions for ships in relation to Lay-up condition. Reference is made to ItoRO no. 23 – Lay Up.

3 Procedures and interpretations

3.1 Security Officer

(former issue no. 037)

The country of domicile of the CSO does not necessarily have to be the Netherlands.

3.1.1 Expertise and responsibility of the CSO

(former issue no. 015)

Reference is made to Policy Rule Safety Seagoing Vessels Art. 2.4 | Training and education of the CSO.

3.1.2 CSO contact details

(former issue no. 059)

To be able to contact ships flying the Dutch flag, in the scope of security (such as a change in the security level), the Dutch authorities must have the contact details and an as complete as possible overview of all CSOs of the ships flying the Dutch flag.

The NSI manages this data and ensures its availability to the KWC. Please submit the contact details of the CSO, including new reports or changes, using the online form "Aanmelden/Wijzigen Gegevens Company Security Officer (CSO) in Dutch)'. Please ensure that any changes are notified to the NSI as soon as possible.

3.1.3 Certification of the SSO

(former issue no. 014)

Reference is made to Article 3.5.8 of the Seagoing vessels crew Regulation for the certification of an SSO.

If an SSO has acquired his/her certificate of proficiency in a country outside the Netherlands, the SSO training course shall have been completed at a training center approved by the Maritime Administration of a country with which the Netherlands has an Agreement in accordance with STCW Code Chapter I, Reg 10.

3.2 Security levels

(former issue no. 010 (& 039))

For ships flying the Dutch flag, the determination of the security level by the Administration, as referred to in regulation XI-2/3.1 of the SOLAS Convention, as well as any supplementary security guidelines and instructions as referred to in Article 4.1 and 4.2 of Part A of the ISPS Code, is effected by the Minister of Infrastructure and Water Management after consulting with the Minister of Justice and Security.

3.2.1 Usual security level

With reference to SOLAS regulation XI-2/3 and the Annex to IMO Circular MSC/Circ.1132 - Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS-Code, section 1.1, unless announced otherwise, ships flying the Dutch flag operate under security level 1.

3.2.2 Changes in security level

Changes in the security level will be communicated to the CSOs by the KWC. Ships registered in the Netherlands must be informed by the CSO and the CSO shall confirm to the KWC that the ships concerned have changed their security level.

3.3 Declaration of Security

(former issue no. 061 (&033)

3.3.1 DoS in general

Reference is made to paragraph 11 – 17 of MSC.1/Circ.1132 - Guidance relating to the implementation of SOLAS chapter XI-2 and the ISPS-Code. In general terms, a DoS should only be drawn up if there is a justified, security-related reason for doing so by a specific ship/port or ship-to-ship contact (see paragraph 13 and also ISPS Part B / 5).

3.3.2 Seagoing ships and inland waterway vessels

A DoS is not mandatory for communication with inland waterway vessels (bunkers, stores, waste transport vessels), as long as:

- the inland waterway vessel has an ISSC, or
- the inland waterway vessel is covered by a PFSP; or
- the SSP of the ship contains procedures for physical security measures in these cases (like monitoring the inland waterway vessel and escorting crew members of the inland waterway vessel, if they are on board the vessel) and these physical security measures are also actually implemented. Noting that the measures were implemented during this contact according to the SSP in the ship's security log is recommended. The same principles apply when loading/unloading inland waterway vessels.

If a DoS is mandatory, but no one on the inland waterway vessel is prepared to draw one up, then the seagoing ship should unilaterally draw up a DoS and establish additional security measures. This may be asked for in the relevant port (PFSO).

3.3.3 Security documentation retention period

(former issue no. 019 (& 020, 051)

Reference is made to Article 31.3 of Regulation Safety Seagoing Vessels.

3.4 Ship certification and verification

Reference is made to Policy Rule Safety Seagoing Vessels Art. 2.1 Certification for registration of existing ships in the Netherlands, and Art. 2.2 Certification of newly built ships.

3.4.1 RSO Auditors

(former issue no. 005)

The need to protect PI must be considered on the content of that information. This includes SSA, SSP and documents detailing the measures put in place.

Reference is made to IACS PR 10 – 7.3; Every (RSO) auditor who participates in SSP approvals or ISPS Code verifications shall be issued with a durable and tamper-proof identity card indicating his or her authorization as a Maritime Security Auditor.

If there are any doubts about the identity of a person who claims to be an RSO auditor, the ship should contact the RSO concerned.

3.4.2 Non-compliance found during a verification for the ISSC

(former issue no. 035)

The CSO is responsible for the performance of alternative measures of a temporary nature, the approved action plan and the performance of permanent measures. The ISSC can be revoked by the RSO if the accepted measures by the RSO are not implemented or the non-conformities become overdue.

3.4.3 Amendments to the approval of SSP / security equipment

(former issue no. 013)

With reference to Policy Rule Safety Seagoing Vessels Art. 2.3 | Changes to previously approved SSPs and security equipment, changes to approved procedures, SSPs and security equipment that influence a ship's security performance must be reported by the CSO to the RSO, for review and approval, before they are implemented.

3.4.4 NSI's interpretations and their implementation

(former issue no. 038)

Changes to the SSP or ship, which become necessary as a result of interpretations of the NSI that are announced after the approval of the SSP, must be implemented before the next intermediate or renewal verification for the ISSC. If the NSI explicitly indicates that these changes must be implemented immediately this has to be done immediately.

3.4.5 Internal reviews / audits of SSP

(former issue no. 030)

With reference to Policy Rule Safety Seagoing Vessels Art. 2.5 | Internal evaluations (reviews/audits) of the SSP, the SSP must be internally reviewed/audited at least once before an intermediate or renewal verification. Records for these activities shall be maintained. With reference to Regulation (EC) 725/2004, Annex II, Part A/9.4.1, personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship.

Actions and measures taken by companies aimed at improving the compliance level and the degree of security awareness on-board their ships are encouraged by the NSI. The annual performance of internal audits can be of assistance in this respect. The 'Self Assessment Questionnaire' as per MSC.1/Circ.1217 - Interim guidance on voluntary self-assessment by companies and company security officers (CSOs) for ship security can be a useful tool for these audits.

If experiences gained from, for example, security drills, give cause to do so, the plan must be changed as soon as possible according to the existing procedure (see section 3.4.3).

3.5 Ensuring readily available security communication between SSO and PFSO

(former issue no. 062)

With reference to paragraph 7.2.7 of Part A of the ISPS Code, and in order to ensure that security communication is readily available, the SSO or a crew member designated by the SSO, shall establish direct contact with the PFSO; such contact may be made by telephone, e-mail, mobile application, or through the physical attendance of the PFSO on board, prior to entering a port or immediately upon arrival at the port facility.

When a ship calls at the same port facility in the same port at least once per month, the requirement to ensure that security communication is readily available:

1. may be fulfilled at least once every three months; and
2. shall be fulfilled in the event of any changes to the contact details or the established means of security communication.

3.6 Access control

(former issue no. 056)

With reference to ISPS Code, Part A, section 7.2.2, access control to the ship is mandatory; however, the ISPS Code does not state that a "gangway watch" is mandatory. Reference is therefore made to Policy Rule Safety Seagoing Vessels Art. 2.6 | Access control for fulfilling the requirement under the ISPS code concerning Access Control. In some countries, more stringent requirements based on local legislation applies and shall be followed (see also paragraph 7 to MSC.1/Circ.1132). The CSO and SSO must take this into account when preparing the voyage.

3.7 Frequency of searches of embarking persons

(former issue no. 034)

Reference is made to Policy Rule Safety Seagoing Vessels Art. 2.7 | Searching individuals who wish to board the ship.

Notwithstanding the obligations of the ship's master to, in accordance with SOLAS XI-2, regulation 8.2, comply with ISPS Code, Part A, Article 9.4.1, and additional guidance by Part B, Article 9.14 – 9.17, the frequency of searching persons embarking the ship are determined as follows:

- Security level 1: As considered necessary by the SSO or the CSO: There are two options:
  1. the SSO or CSO performs a risk analysis, after which the frequency determined is noted in the security records, or
  2. a fixed frequency is specified in the SSP (e.g. 1 in 10 persons).
- Security level 2: at least 1 in 10 persons at random, with a minimum of 1 actual search per port of call;
- Security level 3: all persons.

3.8 SSAS

3.8.1 Security alerts from an SSAS and national contact point

(former issue no. 031 (& 040))

With reference to Regulation Safety Seagoing Ships, Article 31, in the event of an SSAS alert due to an actual security threat, the KWC shall be contacted (preferably by the CSO) as soon as possible by phone. The Netherlands Coastguard Centre can't guarantee fast and efficient processing of security alerts from an SSAS that are sent by e-mail.

3.8.2 Ships of which the SSAS is not functioning properly

(former issue no. 031 (& 040))

In case the SSAS is not functioning properly the R(S)O's needs to be informed by the shipowner; which may consist of 2 societies which needs both to be informed:

- The RO for ship certification (if the SSAS forms a part of the GMDSS equipment); and
- The RSO for ISPS matters.

A security alert from a ship flying the Dutch flag can be communicated to its CSO (and/or Royal Dirkzwager) via other means. The CSO (and/or Royal Dirkzwager) then contacts the KWC to inform them about the Alert.

In such case, the advice is either to:

1. Store a pre-formulated security message (in draft) on the Inmarsat C or Iridium terminal for direct communication;
2. Store a pre-formulated security message (in draft) on e-mail application;
3. Display emergency contact numbers next to the recognized mobile satellite service equipment;
4. The recognized mobile satellite service equipment is pre-programmed, and emergency numbers are available on speed dialing;
5. Familiarize all officers are to use the recognized mobile satellite service equipment;
6. Contacts ships company at regular intervals.

3.8.3 Contact point to follow up SSAS alerts if the CSO is on-board

(former issue no. 058)

This issue is only relevant for companies where the CSO is on-board the ship. Reference is made to Policy Rule Safety Seagoing Vessels Art. 2.8 | Contact for questions pertaining to the SSAS alarm if the CSO is on board.

Please note that where in Art. 2.8 it is stated 'Transport and Water Management Inspectorate (Inspectie Verkeer en Waterstaat)', it should be read as 'Human Environment and Transport Inspectorate (ILT)'. see further section 3.1.2.

Note that for ships without a shore-based contact point or where the appointed contact cannot be reached, the Dutch authorities will assume that each SSAS alert is a real emergency. The Dutch authorities will respond to this alert on that basis, where possible costs may be incurred if the SSAS is falsely used.

3.8.4 Operation and testing of the SSAS

(former issue no. 055 & 036)

Each ship to which SOLAS regulation XI-2/6 applies is fitted with an SSAS. Reference is made to:

- IMO resolution MSC.147(77) (Revised performance standards for ship security alert systems)
- MSC/Circ.1072 - Guidance on provisions of ship security alert systems
- MSC/Circ.1073 - Measures to enhance maritime security

An SSAS is operationally installed and tested according to IACS Procedural Requirement no. 24, paragraphs 2.22, 4.5 and 4,6, whereby during a survey the radio technician who performs the test is not allowed to access the SSP, but limit himself to the SSAS. The frequency of tests of the SSAS must be specified in the SSP. Tests must be readily identifiable as such.

During each operational test of the SSAS, the SSO, or a qualified and authorized substitute, must be present to explain the operation of the SSAS. The CSO is responsible for informing recipients (e.g. the KWC) of test messages in time and the correct confirmation of test message receipt.

If it is established that the SSAS does not comply with the requirements, then the company will contact the RSO and NSI as soon as possible to find a solution.

3.9 Drills and Exercises

(former issue no. 060)

Reference is made to Policy Rule Safety Seagoing Vessels Art. 2.9 | Drills and exercises.

The purpose of these drills and exercises is to test the security system of the company and assure effective coordination, communications, resources available and implementation of SSPs. Relevant authorities may be involved in such exercises, but their participation is not mandatory.

The reports on the exercises must be kept on-board all ships of the company that sail under the Dutch flag. The report obligations are identical to those for the reports on exercises organized by the company itself.

If a ship is unable to provide documentation regarding mandatory exercises during a PSC inspection abroad, then this can be deemed by the PSC as a security deficiency and it may result in detention.

3.10 Ship operating in a non-contracting country

In case the ship is operating in (waters of) a non-contracting country, with regard to SOLAS and the ISPS or (EC) 725/2004, the NSI states that although the ISPS Code is formally not applicable in such country, a Dutch flagged ship however still has to comply to the ISPS requirements and to the approved SSP.

3.11 Ship Security Pre-Arrival Information

Reference is made to SOLAS regulation XI-2/9 and Article 6.1 of Regulation EC 725/2004.

3.11.1 Submitting

Before being allowed to enter a port, seagoing ships must submit SSPI. To avoid unnecessary delays of your ship, it is important to submit the SSPI correct and in time. Take all appropriate actions to avoid unnecessary delays of your ship and submit the security pre-arrival information at least 24 hours prior to arrival. If the voyage time is less than 24 hours, you must submit the information at the latest at the time the ship leaves the previous port. If the port of call is not known or if it is changed during the voyage, please submit the information as soon as you know the port of call.

3.11.2 – UN/LOCODE

The SSPI has to be correct and complete, so with the last 10 calls at Port Facilities, including the UN/LOCODE of the port and the IMO Port Facility number. You can find the IMO port facility numbers in the IMO GISIS database | maritime security | port facilities or ask the shipping agent or PFSO.

Further information about the SSPI-requirements can be found on the ILT-internet site.

3.12 Reporting of denied access to the port facility

When entrance to the port facility for a pre-registered visitor is not granted, and the issue cannot be resolved, via the ship's agent, with a port facility, a notification can be send to the ILT via havenbeveiliging@ilent.nl. Please note that the ILT will not act as an intermediary to obtain immediate access to the port facility, but will include the report during the intergovernmental supervision of the port.