Human Environment and Transport Inspectorate
Ministry of Infrastructure and Water Management

ItoR(S)O no. 25 - SOLAS Chapter XI-2 - Maritime Security (ISPS)

Versie 5

Geldend vanaf: 18-12-2025 tot en met [nog niet bekend].

Documentgegevens

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

Originele versie:
Citeertitel: ItoR(S)O no. 25 - SOLAS Chapter XI-2 - Maritime Security (ISPS)
Permalink: https://puc.overheid.nl/doc/PUC_1178_14

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

Versie en datums:
Versie: 5
Geldend vanaf: 18-12-2025 tot en met [nog niet bekend]
Laatste wijziging: 18-12-2025

Publicatiegegevens:
Uitgever: Inspectie Leefomgeving en Transport
Kanaal: ILT
Vorm: origineel PUC document
Referentienummer: PUC_1178_14
Overige referentienummers: 25
Toegankelijkheid: Intern
Publicatiedatum: 18-12-2025
Taal: en

Verrijking gepubliceerd bij document:
Thema: National Instructions
Hoofdtaak: Koopvaardij / Merchant Shipping

Inhoudsopgave

ItoR(S)O no. 25 - 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 Maritieme Zaken
- DoS: Declaration of Security
- EU:European Union
- ESA: Equivalent Security Arrangement
- GMDSS:Global Maritime Distress and Safety System
- GISIS: Global Integrated Shipping Information System
- 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
- 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
- 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
- STCW:Standards of Training, Certification and Watchkeeping

1 General introduction

The IMO and EU has developed measures for the security of ships and port facilities. To improve the security of ships and port facilities, the (inter)national organizations have 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 instruction is for the application of maritime security legislation (and interpretations) by RSO's for ships flying the flag of the Netherlands.

2 Regulatory framework

The regulatory framework consists of:

- Class agreement dated 03 April 2014;
- 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;
- IACS Procedural Requirements No.24 | ISPS Code Certification (as revised); and
- ItoS – SOLAS Chapter XI-2 - Maritime Security (ISPS).

Please note that there are, besides this ItoR(S)O no. 25, further instructions for vessels in relation to Lay-up condition. Reference is made to ItoRO no. 23 – Lay Up.

3 Procedures and interpretations

3.1 Authorizations

3.1.1 Authozised RSOs

(former issue no. 052)

With reference to:

- ISPS Code, Part A, section 4.3;
- article 4 of the Decree Recognized Organizations Ships Act; and
- the agreement between the Netherlands and the R(S)Os,

the Government of the Netherlands has delegated the security related duties with the exception of ISPS Code, Part A, section 4.3.1 – 4.3.6 to the organizations as stated under article 1 of the Decree Recognized Organizations Ships Act.

3.1.2 RSO Auditor Identification

(former issue no. 005)

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

- For authorized personnel of the RSO which have access to PI, the conduct shall be specified in procedures or job descriptions.
- The inspection of PI shall be conducted by authorized personnel of the RSO only. They shall be screened before starting their duties and the results are recorded, in accordance with the RSO procedures. Requirements for verification of the integrity of authorized personnel of the RSO are to be included in the internal quality procedures of the RSO, and this verification is to be carried out in accordance with such procedures.

With reference to ISPS Code, Part B, section 4.18 (identification documents), before performing an interim, initial, intermediate, renewal or additional verification on-board a ship for the ISSC, an auditor of an RSO must present the following documents to the Master on board:

- a valid passport or driving licence;
- proof of employment; and
- certification conform IACS Procedural Requirement 10 – 7.3 for the performance of approvals and verification.

The documents named are unforgeable. The latter two documents may be integrated into a an ID-card or document.

3.1.3 Protection from unauthorized access or disclosure

3.1.3.1 Transport of information (physical and electronic)

Transmission of PI (hard copy, CD-ROM, DVD, USB-stick or similar) by a company or by an RSO, shall be preferably done by courier or by registered post with tracking facility. Sender and receiver communicate time of dispatch and arrival of physical transport. Preparing for this shipment is carried out by authorized persons appointed and in a neutral and sealed envelope.

In case PI is forwarded through the e-mail it should be encrypted or password protected and passwords (if applicable) are to be sent separately via a different medium.

If an RSO receives unencrypted PI by e-mail, they print it, save it on CD-ROM, DVD, USB-stick or similar and delete mails with PI from computers connected to the network. The sender will be requested to delete the e-mail with PI from their servers.

3.1.3.2 Physical security (buildings, workspace and cabinets)

The office of an RSO has 24/7 access control at the individual level. Registration and identification of individuals in charge shall be ensured. The room with PI is lockable, no access to a room with PI by third parties is permitted without accompaniment of an authorized person.

No PI is left unattended by the auditor at all. All PI (hardcopy, (un)encrypted information) and stamps for official documents are stored in a lockable compartment or safeguarded by the ISPS auditor.

3.1.3.3 Information management

Information carriers (CD-ROM, DVD, USB-stick or the like) are used so that the information shall not be accessible to unauthorized persons (e.g. by using encryption).

An auditor shall not make more reproductions (hard copy and electronic) than necessary for the review. After the review no PI or reproductions may be kept (hardcopy or electronically) and they are to be deleted / shredded as appropriate.

For archiving purposes only the following information may be stored unprotected: front page, table of contents, page revision (with stamps).

3.1.3.4 Security breach

The RSO shall ensure that the NSI is informed of security events and weaknesses related to information security (i.e. the unauthorized access, use- or manipulation of information) with an initial notification within 24 hours of noticing the event. The RSO is responsible for taking corrective action in time.

3.2 Ship certification process

(former issue no. 041 & 042)

3.2.1 3.2.1 Existing ships transferring to the Netherlands' register

Reference is made to Policy Rule Safety Seagoing Vessels Art. 2.1 | Certification for registration of existing ships in the Netherlands. This applies to both ships flagging in with- and without an ISSC.

3.2.2 Newly built ships

Reference is made to Policy Rule Safety Seagoing Vessels Art. 2.2 | Certification of newly built ships.

3.2.3 'Green Stamp' ships

(former issue no. 057 (& 029))

Ships having a declaration based on Resolution A.791(19) regarding the application of the International Convention on Tonnage Measurement of Ships 1969 to existing ships of less than 500 GT ('Green Stamp' ships), are not necessarily exempted from the obligation of having an ISSC.

The criterion to decide whether a ship should comply with the regulations of SOLAS Chapter XI-2 and Part A of the ISPS Code is the gross tonnage of a ship that is determined according to the ITC'69.

3.2.4 ESA

A ship may decide to make up an ESA, in compliance with SOLAS regulation XI-2/13, sub 6. Such security measures must be at least as effective as those prescribed in SOLAS Chapter XI-2 or the ISPS-code, Part A.

ESAs do not allow SOLAS ships to avoid full compliance with the requirements of the Maritime Security Measures. The NSI reports an ESA to the IMO by use of GISIS.

3.2.5 Installation of the SSAS

(former issue no. 055 & 036)

Each ship to which SOLAS regulation XI-2/6 applies is fitted with an SSAS. Herewith, 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 inspected according to:

- IACS Procedural Requirement no. 24, paragraphs 2.22, 4.5, 4,6, 6.1, 6.4, 6.5 and 7, and
- IACS Unified Interpretation SC 194, taking into account the following clarification regarding operational testing:
  I. the SSAS must be disconnected from the GMDSS system if operationally testing is not possible during the initial survey of an SSAS that is connected to the GMDSS system;
  II. when operationally testing an SSAS, the radio technician who performs the test will not access the SSP, but limit himself to the SSAS;
  III. an SSAS shall comply with the performance standard IEC60945 and the relevant specifications regarding radio communications as contained in the Radio Regulations and relating to the International Convention regarding Telecommunications (ITU).
  IV. 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 Coastguard Centre) of test messages on time and the correct confirmation of test message receipt.

If it is established that the SSAS does not comply with the requirements, then:

- the RSO will report this to the Inspectorate as soon as possible;
- during a radio survey: the radio safety certificate referred to in Article 5, sub 1.c. of the Ships Decree 2004 will be endorsed as long as the GMDSS system equipment (as per SOLAS chapter IV) functions correctly.

In the event that the RSO auditor does not find any SSAS operational test results during a verification audit for the ISSC, then, before the audit is finished:

- the SSO must perform an operational test of the SSAS and log a report thereof ;
- a certified radio technician must perform an operational test and log a report that the SSAS complies with SOLAS regulation XI-2/6 and forms a part of a GMDSS system that complies with the regulations of SOLAS Chapter IV.

3.2.6 Non-compliance found during a verification for the ISSC

(former issue no. 035)

If an RSO auditor determines that the ship does not comply with the relevant provisions of chapter XI-2 of the SOLAS Convention or the mandatory parts of the ISPS Code during a verification for the ISSC, then the following action is to be taken:

1. initial and renewal audit: non-compliances need to be rectified to the satisfaction of the RSO before the ISSC will be issued.
2. interim and intermediate audits: to reach the required security level with alternative measures in the short term, the CSO and/or SSO must propose alternative measures of a temporary nature. They must be presented to the RSO for approval. The RSO assesses the alternative measures and the CSO and/or SSO implements the temporary measures. To achieve and maintain the security level with structural measures for the long term, the CSO and/or SSO draft an action plan, including a time schedule, and present this to the RSO for approval. The RSO assesses the permanent measures and the CSO and/or SSO implements them as permanent measures and informs the RSO about them.

With reference to Article 5.5 of the agreement between the Netherlands and the RSOs, Major failures or Major Non-conformities (as defined and referred to in IACS Procedural requirement no. 24 are considered as severe non-compliances of a specified requirement and when found during a verification are to be communicated to the NSI immediately by e-mail (nsi-tez-kv@ilent.nl).

The ISSC can be revoked if the accepted measures by the RSO are not implemented or the non-conformities become overdue. Besides the NSI, the RSO also has this authority. The RSO reports any invalidation of the ISSC the NSI.

3.2.7 Verification of changes to the SSP

(former issue no. 007)

With reference to ISPS Code, Part A, section 19.1(.4), the RSO assesses and inspects the SSP or changes made to an SSP that was approved earlier. Any rectification of shortcomings/deficiencies will be verified by the RSO. The evaluation method for changes to an SSP that require the RSO's approval under all circumstances can be found in table 2.1 of the Policy Rule Safety Seagoing Vessels Art. 2.3 | Changes to previously approved SSPs and security equipment.

3.2.7.1 Cross reference Cross reference between SSP and SMS

For the verification of changes to the SSP, special reference is made to the workaround for cross reference between SSP and SMS | cyber security procedures.