Inspectie Leefomgeving en Transport
Ministerie van Infrastructuur en Waterstaat

Consolidated interpretations of the Security Rules and Regulations by the Netherlands Shipping Inspectorate

Version 3.3

Date	1 February 2021
Status	DEF

Colophon

Human Environment and Transport Inspectorate
Netherlands Shipping Inspectorate

Contact Client Contact Centre
T +31 (0)88-489 0000
E-mail via contact form on website www.ilent.nl

Version 3.3

Version	Prepared by	Date of adoption
1.0 to 1.9.	B.O. Maltha	2004 - 2007
2.0 to 2.4.	B.O. Maltha/J. Schot	2009 - 2011
3.0	J. Borsten	16 April 2012
3.1	J. Borsten	27 April 2012
3.2	J. Borsten/J.M. van Waesberghe	6 June 2019
3.3	J.M. van Waesberghe	1 February 2021

Change management:

3.0 → 3.1	Issue 031 (& 40): DCC general number change: +31 (0)70 456 8555 Issue 030:
3.1 → 3.2.	General information: General textual editing. References to Easy Rules are replaced by references to NeRF. Various changes in the links to internet sites. Name changes from IVW to ILT and I&M to I&W. Issue 005: RSO auditors can identify themselves with unforgeable proof of authority, pursuant to IACS Procedural Requirement 10, for the purpose of performing inspections to verify eligibility for ISSC. Issue 014: *Regeling certificering scheepsbeveiligingsfunctionarissen* (Ship's Security Officer Certification Regulation) replaced by *Regeling Zeevarenden* (Seafarers' Regulation). Issue 059: change in P.O. Box number and website link. Issue 031: SSAS procedure and change in DCC telephone number. Issue 052: date Class agreement and RSOs summary. New Issue 062: an SSO must test communication with PFSO.
3.2 → 3.3	Issue 062: Revision of text based on input from RSO's.

If questions are raised regarding the content, the original version of the regulatory framework as published in the Netherlands language prevails.

Contents

Introduction

Following the tragic events of 11 September 2001, the International Maritime Organisation (IMO) unanimously agreed, in the same year, to develop new measures for the security of ships and port facilities.

To improve the security of ships and port facilities, the IMO adopted Chapter XI-2 (special measures to enhance maritime security) of the International Convention for the Safety of Life at Sea (SOLAS Convention) and the International Ship and Port Facility Security (ISPS) Code in December 2002. Chapter XI-2 of the SOLAS Convention and the ISPS Code entered into force on 1 July 2004 and it applies to all passenger ships and cargo ships with gross tonnage of 500 tons or more, which are engaged on international voyages, and port facilities serving such ships engaged in international voyages. These instruments to improve the security of ships engaged in international trade and the associated port facilities contain mandatory provisions.

The EU has adopted Regulation (EC) No. 725/2004. This regulation alters the scope of several of the provisions of the ISPS Code in the European Community. The same applies to the provisions in the ISPS Code regarding the recommendations, of which several have acquired a mandatory character in the European Community. The regulation took effect on 19 May 2004 and was made applicable from 1 July 2004.

Additional information can be found on, for example, the websites of the *Inspectie Leefomgeving en Transport (ILT)*, (Human Environment and Transport Inspectorate), the *Ministerie voor Infrastructuur en Waterstaat* (Ministry of Infrastructure and Water Management), the EU, the IMO and the *Koninklijke Vereniging van Nederlandse Reders (KVNR)* (Royal Association of Netherlands Shipowners).

Current contact information on the security of ships and port facilities can be found on the website www.ilent.nl.

1. Supervision

The supervision of Dutch merchant shipping to determine compliance with the security measures required by ships and port facilities, as prescribed in Chapter XI-2 of the SOLAS Convention, ISPS Code and Regulation (EC) No. 725/2004, is tasked to the Human Environment and Transport Inspectorate (the Netherlands Shipping Inspectorate).

For questions and additional information, please contact the Client Contact Centre by phoning the general number +31 88 489 0000 (24 hours) or by using the contact form on the Inspectorate's website.

2. Interpretations

EU Regulation 725/2004 (incl. Annex I: SOLAS Chapter XI-2, Annex II: Part A of the ISPS Code and the Annex III, Part B of the ISPS Code with mandatory parts for the EC) contain provisions that give the member states some freedom of interpretation. These Interpretations endeavour to clarify them. The Human Environment and Transport Inspectorate recommends that you regularly check its website for new versions:www.ilent.nl.

The overview has grown in size over time and various new versions have been published. The information is divided into a number of chapters:
1. Procedures and other information;
2. Ministerial regulations; matters that have been laid down in various regulations;
3. Policy rules; matters laid down in the Policy Rules for the safety of seagoing ships;
4. Other interpretations.

The decision was taken to retain the old system of numbering issues, since various users refer to them in internal publications. We recommend that you carefully check the various chapters and subjects, as some numbers have lapsed. If you have any further questions, please contact the Inspectorate or, perhaps, present your question(s) to your Recognised Security Organisation (RSO) or the *Koninklijke Vereniging van Nederlandse Reders (KVNR)* (Royal Association of Netherlands Shipowners).

3. Procedures and other information

The issues below provide further information about procedures and the like, as per ISPS Code.

Issue No.:	Subject:
005	**RSO Auditor Identification**

Before performing an interim, initial, intermediate, renewal or additional verification on-board a ship for the International Ship Security Certificate (ISSC), an auditor of a Recognised Security Organisation (RSO) must present the following documents:

- a valid passport or drivers licence;
- proof of employment; and
- certification conform IACS Procedural Requirement 10 for the performance of an initial, interim, additional or renewal verification of the ISSC .

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

Issue No.:	Subject:
007	**Applying for an International Ship Security Certificate (ISSC)**

- The interim, initial, intermediate, renewal or additional verifications for the ISSC are performed by a Recognised Security Organisation (RSO). An ISSC (including an interim ISSC) is issued by the RSO.
- The RO assesses and inspects the Ship Security Plan (SSP) or changes made to an SSP that was approved earlier.
- The on-board verification will be done an RSO auditor.
- Any rectification of shortcomings/deficiencies will be verified by the RSO.
- Issue of ISSC or interim ISSC

Issue No.:	Subject:
010 (&39)	**Security Levels**

- Unless announced otherwise, the security level is 1 for ships registered in the Netherlands (Also refer to IMO Circular MSC/Circ.1132).
- For ships registered in the Netherlands, the determination of the security level, as referred to in regulation XI-2/3.1 of the SOLAS Convention, as well as any supplementary security guidelines as referred to in Article 4.1 of Part A of the ISPS Code, and of any instructions as referred to in Article 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. Changes in the security level must be communicated to the Company Security Officers (CSOs) by the Coastguard Centre (KWC) in Den Helder (Also refer to issue no. 059). The ships registered in the Netherlands must be informed by the CSO and the CSO must confirm to the

Coastguard Centre (KWC) that the ships concerned have changed their security level.

Issue No.: **033**	Subject: **Use of Declaration of Security (DoS)**
• Paragraphs 11 to 17 of IMO Circular MSC/Circ.1132 apply to ships that sail under the Netherlands flag and to which the ISPS Code applies. • See issue no. 019 for the DoS retention time.	

Issue No.: **035**	Subject: **An RSO finds shortcomings during an interim, initial, intermediate, or renewal verification for the International Ship Security Certificate (ISSC)**
• 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 an initial, intermediate, interim, or renewal verification for the International Ship Security Certificate (ISSC), then the following action is to be taken: 1. As the initial and renewal audit requires full compliance the Non-compliances need to be rectified to the satisfaction of the RSO before the ISSC will be issued. 2. For 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. • The RSO reports the shortcoming found to the Inspectorate pursuant to Article 5.5 of the agreement between the Netherlands and the RSOs, as referred to in Article 3 of the *Regeling erkende organisaties Schepenwet* (Recognised Organisations Shipping Act Regulation). • 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 if the accepted actions by the RSO are not implemented or the non-conformities become overdue. Besides the Inspectorate, the RSO also has this authority from 1 August 2006. The RSO reports any invalidation of the ISSC the Inspectorate.	

Issue No.: **037**	Subject: **Residence of the CSO**
The CSO may be domiciled outside the Netherlands.	

Issue No.: **048**	Subject: **Application for Continuous Synopsis Record**

	(CSR)
• With the exception of the ships indicated in SOLAS regulation I/3, a Continuous Synopsis Record (CSR) may be issued for each ship to which chapter I of the SOLAS Convention applies. A CSR application form is available from the website of the Inspectorate. • This application form can also be used for flagging out (signing out of the Netherlands registry). • The Inspectorate issues a CSR document based on a model form drafted by the IMO (IMO resolution A.959(23) as amended with the IMO Circular MSC.198(80)). • The original CSR documents (comprising form 1, 2 and 3) must be kept on-board for as long as the ship is in service. • If an existing ship is registered in the Netherlands, and the previous flag State does not send the previous CSR document on time, then the ILT will issue a new CSR according to the instructions of the IMO Resolution A.959(23) as amended with IMO Circular MSC.198(80).	

Issue No.:	Subject:
049	**Ships registered in Curaçao, Aruba or Sint Maarten**
Please contact the maritime authorities in Curaçao, Aruba or Sint Maarten. https://english.ilent.nl/themes/s/security/contact-details-ship-security	

Issue No.:	Subject**:**
055 & **036**	**Ship Security Alert System (SSAS)**

- Each ship to which SOLAS Chapter XI-2 applies is fitted with a Ship Security Alert System (SSAS) pursuant to regulation 6 of SOLAS Chapter XI-2.
- Relevant documentation regarding the requirements of a SSAS:
  - ISPS Code
  - SOLAS Chapter XI-2, regulation 6
  - IMO resolutions MSC.136(76) and MSC.147(77)
  - IMO Circulars MSC/Circ.1072 (IMO Circular MSC/Circ.1073 may also be relevant)
- If uncertainty or inconsistency exists regarding the applicability of IMO resolution MSC.147(77) (Revised performance standards for ship security alert systems IMO resolution MSC.136(76) (Performance standards for a ship security alert system)), then the latter prevails.

SSAS operational requirements:

- The Inspectorate will not issue any type approval for SSAS.
- An SSAS is operationally tested according to:
- IACS Procedural Requirement no. 24, paragraphs 2.25, 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:
  - the SSAS must be disconnected from the GMDSS system if operationally testing the SSAS is not possible during the initial survey of a SSAS that is connected to the GMDSS system, which complies with the regulations of SOLAS Chapter IV;
  - when operationally testing a SSAS, the radio technician who performs the test will not access the SSP, but limit himself to the SSAS;
  - an SSAS complies 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).
- During each operational test of the SSAS, the SSO, or a qualified and authorised 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 as named in SOLAS regulation XI-6, then:
  - the RSO will report this to the Inspectorate as soon as possible;
  - the company will contact the Inspectorate as soon as possible to find a solution;
  - during a radio survey: the safety certificate referred to in Article 5 of the Ships Decree 2004 will be endorsed if the GMDSS system functions correctly.
- In the event that the RSO auditor does not find any SSAS operational test results during an interim, initial, intermediate, additional or renewal verification audit for the International Ship Security Certificate (ISSC), then, before the audit is finished:
  - the SSO must perform an operational test of the SSAS and log a report there off.;

- 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.

Issue No.: **057** (&29)	Subject: **"Green Stamp" Ships**

- Ships having a declaration based on IMO resolution A.791(19) regarding the application of the International Convention on Tonnage Measurement of Ships 1969 on existing ships with a gross register tonnage (GRT) of less than 500 tons ("Green Stamp" ships), are ***NOT*** necessarily exempted from the obligation of having an International Ship Security Certificate (ISSC) (IMO Circular MSC/Circ.1157).
- 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 International Convention on Tonnage Measurement of Ships 1969.

Issue No.: **059**	Subject: **CSO contact details**

To be able to contact Netherlands registered ships with regard to a change in the security level, or other instructions in the scope of security, the Dutch authorities must have the contact details and an as complete as possible overview of all Company Security Officers (CSOs) of the ships registered in the Netherlands. The following particulars are required:

- CSO's name (all CSO's names if more than one CSO in one company)
- Work telephone number(s) of CSO(s);
- Mobile telephone number(s) of CSO(s) (24 hours);
- Home telephone number(s) of CSO(s);
- Email address(es) of CSO(s) (24 hours);
- Company's name and address;
- Company's telephone number;
- Company's fax number;
- Other relevant particulars (e.g. substitute CSO(s));
- Name of relevant ship(s) concerned;
- Call sign of relevant ship(s) concerned; and
- IMO number of relevant ship(s) concerned;

The Inspectorate manages this data and ensures its availability to the Coastguard Centre. Changes may be made by using the form "Aanmelden/Wijzigen Gegevens Company Security Officer (CSO)" ('Register/Change Company Security Officer Contact Details'). This form can be found on the ILT website: https://english.ilent.nl/themes/f/forms-merchant-shipping/documents/forms/2016/12/22/form-report-change-contact-details-company-security-officer-cso

Changes can also be sent:
By post: ILT
Postbus 16191
2500 BD The Hague, The Netherlands
By e-mail: csodata@ilent.nl
PLEASE NOTIFY THE INSPECTORATE OF ANY CHANGES IN GOOD TIME!

4. Ministerial Regulations

The following issues have been laid down and published in ministerial regulations. Reference is made to the relevant ministerial regulation per subject.

Issue No.: **004 (&046)**	Subject: **EU Regulation and Interpretations**
Ships registered in the Netherlands must comply with Regulation (EC) No. 725/2004 (See also Article 31.2 of the Regeling Veiligheid Zeeschepen (Seagoing Ships' Safety Regulation). The definitive version of the regulation can be found in NeRF or via the Inspectorate's website: https://puc.overheid.nl/nsi/doc/PUC_2318_14/1/ The Dutch interpretation of the provisions of Regulation (EC) No. 725/2004, the ISPS Code and SOLAS Chapter XI-2 prevails over a differing interpretation of a RSO. If a dispute arises between a shipowner and a RSO that cannot be resolved between them, then one can contact the Inspectorate (+31 (0)88 489 0000/24 hours). The findings of the RSO will be considered by the Inspectorate as advice.	

Issue No.: **014**	Subject**:** **Certification of the Ship Security Officer (SSO)**
See Regeling Zeevarenden (Seafarers Regulation), as published in the Government Gazette of 2 May 2014, no. 11484: Article 8.38: Before a Ships Security Officer *(SSO)* certificate can be issued: a. the applicant must satisfy regulation VI/5, paragraph 1.1, of the Annex to the International Convention on Standards of Training, Certification and Watch-keeping for Seafarers (STCW), and; b. the applicant must have successfully concluded a course and training recog-nised by Our Minister that complies with section A-VI/5, paragraphs 1 to 4, of the STCW Code. Article 41, paragraph 1, of the Maritime Crews (Merchant Marine and Sailing Ships) Decree: "Crew members that are appointed as a Ship Security Officer (SSO) must have a Ship Security Officer Certificate." Non-Dutch SSOs are Ship Security Officers according to Article 8.38, if the SSO acquired his/her certificate in a country with which the Netherlands has concluded a bilateral agreement regarding mutual recognition of courses and training. The countries with which the Netherlands has concluded a bilateral agreement can be seen on the website: https://english.ilent.nl/themes/m/merchant-shipping-crew/documents/publications/2015/03/02/memberstates-with-bilateral-agreement-on-training RSOs monitor this for on-board verification and SSP approval. Certificate applications can be submitted to the bodies specified therein.	

Issue No.:	Subject:
019 (& 20 & 51)	**Records and Declaration of Security (DoS) retention period**

Records retention time
All records specified in paragraph 10.1 of Annex 2 of EC regulation 725/2004 and Part A of the ISPS Code shall be kept on-board for a minimum period of 3 years, pursuant to Article 31.3 of the Seagoing Ships Safety Regulation.

DoS retention time
A DoS must be retained for a minimum of 3 months, or for as long as needed to cover the period of the last 10 calls at Port Facilities , in accordance with Article 31.3 of the Seagoing Ships Safety Regulation (see also IMO Circular MSC/Circ.1132, paragraph 17).

Issue No.:	Subject:
031 (&40)	**Security alerts from a Ship Security Alert System (SSAS) and national contact point**

Ships registered in the Netherlands
Security alerts from a SSAS of a ship registered in the Netherlands must be transmitted (possibly via the CSO) to the Netherlands Coastguard Centre in Den Helder.

- Phone number: +31 (0)900 - 0111
- Fax number +31 (0)223 - 658 358 (24/7)
- Email address: ccc@kustwacht.nl

The Netherlands Coastguard Centre CANNOT guarantee fast and efficient processing of security alerts from an SSAS that are sent by e-mail.
(see Article 31.1 of the Seagoing Ships Safety Regulation)

Ships of which the SSAS is not functioning properly:
In this case, a security alert from a ship registered in the Netherlands can be communicated as follows:

- The ship can notify its shipping company/CSO (or Dirkzwager),
- The shipping company/CSO (or Dirkzwager) then contacts the Departmental Crisis Coordination Centre (DCC) of the Ministry of Infrastructure and Water Management.

Telephone numbers of the DCC:

- General number: +31-(0)88 797 0222
- The emergency number is: +31-(0)800 351 8700 (24/7)

Contact point
Regulation XI-2/7.2 makes it mandatory to appoint a contact point, to which ships in the (proximity) of the territorial sea of a State can turn for advice or assistance in the field of security or to which those ships can report any concerns regarding security-related issues. In both cases, the Coastguard Centre was chosen, which institution is also responsible for outgoing message traffic tasks in the field of security. (see explanatory notes to Art. 31 of the Seagoing Ships Safety Regulation, as published in the Government Gazette of 23 December 2004, no. 248).

Issue No.:	Subject:
052	**Recognised Security Organisations (RSOs)**

In the agreement between the Netherlands and the RSOs, as referred to in Article

3 of the Recognised Organisations Shipping Act Regulation, the following organisations are authorised to perform inspections and verifications for the International Ship Security Certificate (ISSC) for ships sailing under the Dutch flag:

- American Bureau of Shipping (ABS);
- Bureau Veritas (BV);
- Det Norske Veritas (DNV) (As of 1 March 2021 name change from DNV GL to DNV);
- Indian Register of Shipping (IRClass);
- Lloyd's Register (LR);
- Nippon Kaiji Kyokai (ClassNK);
- Registro Italiano Navale (RINA).

5. Policy Rules

The national policy rules regarding ship security measures against terrorism, piracy, criminality and vandalism are contained in Article 2 to Article 2.9 of the Marine Shipping Safety Policy Rules and they apply to ships sailing under the Dutch flag and to which the regulations of SOLAS Chapter XI-2, the ISPS Code and Regulation EC/725/2004 apply.

The Marine Shipping Safety Policy Rules (Dutch: Beleidsregel veiligheid zeeschepen) can be found at: https://puc.overheid.nl/nsi/doc/PUC_2047_14/1/

Issue No.: **013**	Subject: **Amendments to the approval of SSP / Security equipment**
Also refer to Article 2.3 of the Marine Shipping Safety Policy Rules (in NeRF). Changes to approved procedures, SSPs and Security Equipment that influence a ship's security performance must be reported to the RSO before they are implemented. The RSO will decide what procedure must be followed per case, based on the guidelines provided by the Inspectorate. https://english.ilent.nl/themes/s/security/documents/publications/2006/07/26/changes-tot-ship-security-plans	

Issue No.: **015**	Subject**:** **Company Security Officer (CSO)**
Also refer to Article 2.4 of the Marine Shipping Safety Policy Rules (in NeRF). The CSO must possess the expertise and skills necessary to correctly perform the tasks specified in ISPS Code, Part A, Art. 11 (ISPS Code, Part A, Art. 13.1). To this end, the CSO must at least be able to prove that he/she has successfully completed training in accordance with ISPS code, Part B, Art. 13.1.	

Issue No.: **030**	Subject: **Internal reviews/ audits of SSP**
Also refer to Article 2.5 of the Marine Shipping Safety Policy Rules (in NeRF). To comply with ISPS Code, Part B, Art. 1.12 and 9.2.6, the SSP must be reviewed/audited between two consecutive verifications or re-inspections at least once before an intermediate or renewal verification. The records about these activities shall be maintained. 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 issue 13). 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 Inspectorate. The annual performance of internal audits can be of assistance in this respect. The "Self Assessment Questionnaire" developed by IMO and the EU can be a useful tool for these audits. This IMO Circular	

(MSC.1/Circ.1217, interim guidance on voluntary self-assessment by companies and company security officers (CSO's) for ship security) can be found via IMO-Docs on www.imo.org.

Issue No.:	Subject:
034	**Frequency of searches of embarking persons**
Also refer to Article 2.7 of the Marine Shipping Safety Policy Rules (in NeRF). 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 Part B, Article 9.15, the frequency of searching persons wishing to board the ship are determined as follows. By *security level*: 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 embarking persons). Security level 2) at least 1 in 10 embarking persons at random, with a minimum of 1 actual search per port of call. Security level 3) everyone, all embarking persons. The above applies, with reference to that stated in SOLAS XI-2, regulation 8.	

Issue No.:	Subject:
041	**Certification when registering existing ships in the Netherlands**
Also refer to Article 2.1 of the Marine Shipping Safety Policy Rules (in NeRF). If the company remains the same, the procedure is as follows: • The SSP must be approved by a RSO appointed by the Netherlands, taking into account the specific Dutch interpretations. • If the RSO recently approved the SSP for another flag, this RSO can, in principle, suffice with a check limited to specific Dutch interpretations. • An on-board verification must be performed in accordance with the instructions and interpretations of the NSI . In principle, this can comprise an earlier verification for another flag and an extra verification limited to the specific Dutch requirements. A long-term certificate can be issued if the above procedure is followed correctly. This applies to both ships flagging in (refers to the process of adding a vessel to the national registry) with and without an ISSC. If a new company takes control of the ship: • A CSO must be appointed by the new company. • This CSO must complete a new SSA and draft a new SSP. The CSO may reuse parts of the old SSP if applicable. However, this does not guarantee certification. • If one satisfies the conditions of Article 19.4.2 of Part A of the ISPS Code, an interim certificate may be issued by the RSO for 6 months on the grounds of	

Article 19.4.1 of Part A of the ISPS Code if problems arise due to a lack of time owing to flagging in. .

Issue No.:	Subject:
042	**Certification for new ships**
Also refer to Article 2.2 of the Marine Shipping Safety Policy Rules (in NeRF). If one satisfies the conditions of Article 19.4.2 of Part A of the ISPS Code, an interim certificate may be issued by the RSO, valid for 6 months, on the grounds of Article 19.4.1 of Part A of the ISPS Code.	

Issue No.:	Subject:
056	**Access control**

Also refer to Article 2.6 of the Marine Shipping Safety Policy Rules (in NeRF).

- Access control is mandatory under SOLAS security requirements (ISPS A 7.2.2).
- However, the ISPS Code does not state that a "gangway watch" is mandatory.

The access control, does not necessarily means using a "gangway watch". Other options include, for example, a lookout on the bridge or on deck, security cameras or external security personnel. The key point is that someone is always monitoring access to the ship and visitors are approached upon boarding the ship and instructed to identify themselves and indicate the purpose of their visit.

The SSP should reflect the above and the RSOs appointed, who operates on behalf of the Dutch authorities, should only approve plans in accordance with ISPS A 7.2.2. and the EC mandatory sections of ISPS Code part B. If an RSO has approved plans that are not compliant, this situation should be corrected immediately.

In some countries, more stringent requirements based on local legislation apply. The CSO and SSO must take this into account when preparing the voyage.

Issue No.:	Subject:
058	**Contact point to follow up SSAS alerts <u>if the CSO is on-board</u>**

<u>This issue is only relevant for companies where the Company Security Officer (CSO) is domiciled on-board the ship</u>

Also refer to Article 2.8 of the Marine Shipping Safety Policy Rules (in NeRF).

- If the Coast Guard Centre receives an alert via a Ship Security Alert System (SSAS), it will inform the Departmental Crisis Coordination Centre (DCC) and the CSO will be contacted to obtain further information and establish whether or not it concerns a false alert. This is not possible if the

CSO is also the ship's master, as it is not the intention that the Dutch authorities contact the ship directly after receiving an SSAS alert (see MSC Circular 1073, particularly Art 2.4.2 of the Annex, concerning the so-called "Covert Alert").

- In this case, there is a need for a shore-based contact point.
- This can be the contact point as required by the mandatory contact point registration legislation, but also an external organisation or person. No party has exclusive rights in this respect.
- There has to be a written agreement between the ship and the party acting as contact point, which specifies that the contact point is available at all times for assistance in the event of a security alert. The contact point must be able to supply to the Dutch authorities as much relevant information as possible regarding the ship (ship type, cargo, position, crew numbers, the presence of dangerous substances, etc.).
- The Coastguard Centre must be informed of the SSAS contact point. The contact details of this contact point must be registered with the Human Environment and Transport Inspectorate (ILT). It in turn informs the Coastguard Centre. See issue no. 59.
- For ships without a shore-based contact point, 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 SASS is falsely used.

Issue No.:	Subject:
060	**Drills and Exercises**

Also refer to Article 2.9 of the Marine Shipping Safety Policy Rules (in NeRF).

Drills
Drills must be performed on-board, according to the requirements of ISPS, Part A, Paragraph 13.4 and Part B, paragraph 13.6. The SSO is the person who holds primary responsibility for its implementation.

Exercises:
"Exercises" are not the same as "drills" and they must be held annually (each calendar year) with no more than 18 months between them, according to the requirements of ISPS Part A, paragraph 13.5 and Part B paragraph 13.7.
The organisation of these exercises is in principle the responsibility of the company (in this case the CSO). .
The purpose of these exercises is to test the security system of the company and assure effective coordination, communications, resources available and implementation of SSPs.
More than one company ship (if applicable), but not all ships of the same company have to be involved in a specific exercise.
The results of these exercises have to be shared with all other ships of the same company that sail under the Dutch flag. These results must be discussed on-board each ship, and a record of this must be logged in the ship's log. Moreover, any improvement identified during the exercises where applicable, shall be

implemented on all ships of the company sailing under the Dutch flag.
The reports on the exercises must be kept on-board all ships of the company that sail under the Dutch flag.

Relevant authorities may be involved in such exercises, but their participation is not mandatory. Authorities are certainly encouraged to perform their own exercises.
If a CSO participates in such an exercise, this counts as an annual mandatory exercise (see ISPS, Part B, paragraph 13.8). The report obligations are identical to those for the reports on exercises organised by the company itself.
If, when asked, a ship is unable to provide documentation regarding the mandatory exercises (for example during an intermediate verification) to the Inspectorate, or an RSO acting on its behalf, the ISSC may be revoked.

If a ship is unable to provide documentation regarding mandatory exercises (Exercises & Drills) during a Port State Control (PSC) inspection abroad, then this can be deemed by the PSC organisation as a security deficiency and it may result in detention.

6. Other interpretations

Issue No.:	Subject:
038	**Interpretations and their application**

- Changes to the SSP or ship, which become necessary as a result of interpretations of the Dutch authorities that are announced later, must be implemented before the next intermediate or renewal verification for the International Ship Security Certificate (ISSC).
- If the Inspectorate explicitly indicates that these changes must be implemented immediately this has to be done immediately.

Issue No.:	Subject:
061 (see also issue 33)	**Declaration of Security (DoS) Use**

DoS in general
A ship must comply with a request from a port facility to draw up a DoS. However, a port facility, or another ship (by ship-to-ship contact), is not obliged to comply with a similar request from a ship, but need only confirm receipt of the request.

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.
In any event, drawing up a DoS is recommended:
- in the circumstances specified in article 5.2 of Part A of the ISPS Code*.
- in situations that are not covered by the SSP and/or PFSP.
- if the contact is with a non-ISPS ship that is transporting hazardous substances.

(See Chapter 5 of Part A and Chapter 5 of Part B of the ISPS Code and IMO Circular MSC/Circ.1132).

Contact between ships and inland vessels
A DoS is NOT mandatory for communication with inland vessels (bunkers, stores, waste transport vessels), so long as:
- the inland vessel has an International Ship Security Certificate (ISSC), or
- the inland vessel is covered by a Port Facility Security Plan (PFSP); or
- the Ship Security Plan (SSP) of the ship contains procedures for physical security measures in these cases (like monitoring the inland vessel and escorting crew members of the inland 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 vessels.

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

* Article 5.2 of Part A of the ISPS Code states that a ship can submit a request to draw up a DoS, when:

.1 the ship is operating at a higher security level than the port facility or another ship, with which it is cooperating;
.2 an agreement regarding a DoS exists between contracting States regarding certain international voyages or specific ships used for them;
.3 there has been a security threat or security incident involving the ship or port facility, as applicable;
.4 the ship is in a port where having or implementing an approved Port Facility Security Plan (PFSP) is not mandatory;
.5 the ship conducts ship-to-ship activities with another ship that is not obliged to have or implement an approved Ship Security Plan (SSP).

Issue No.:	Subject:
062	**SSO must have the contact details of the PFSO at each Port Facility**

Also refer to ISPS Code A, Article 7.2.7 (in NeRF).

A means to satisfy this requirement is to contact the PFSO directly in order to verify that security communication is readily available. This may for instance be carried out by verification of pre-arrival ISPS information provided by the vessel's agent and can be done by phone, e-mail, app's, on-board attendance by PFSO, etc; This will result in establishing that availability of up-to-date security communication details is ensured at all times. Contacting of the PFSO may be carried out by the SSO or an appointed crew member and is to take place within 24 hours prior to arrival or immediately after arrival in the port facility. In this respect it should be noted that, without replacing the real test described above, the CSO can assist the SSO in ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officers. Note: For vessels that attend the same port facility on a regular basis (fixed timetable or at least once every month), the minimum frequency to verify security communication is set on a quarterly basis, or reconfirmed when changes to security communication details occur. The objective of this interpretation is to ensure full compliance with article 7.2.7 of the ISPS Code at all times.

Most important abbreviations:

Abbreviation	Meaning	English translation
ISSC	International Ship Security Certificate	
ISPS	International Ship & Port Facility Security Code	
ILT	Inspectie Leefomgeving en Transport (formerly IVW)	Human Environment and Transport Inspectorate
RSO	Recognized Security Organization	
SSA	Ship Security Assessment	
SSP	Ship Security Plan	
SSAS	Ship Security Alert System	
SSO	Ship Security Officer	
CSO	Company Security Officer	
CSR	Continuous Synopsis Record	
AIS	Automatic Identification System	
ASA	Alternative Security Agreement	
DA	Designated Authority	
DCC	Departementaal Crisis Coördinatiecentrum	Departmental Crisis Coordination Centre
EU	European Union	
ILO	International Labour Organisation	
IMO	International Maritime Organisation	
MSC	Maritime Safety Committee (IMO)	
PFSO	Port Facility Security Officer	
PFSP	Port Facility Security Plan	
PSO	Port Security Officer	
KWC	Kustwacht Centrum Den Helder	Coastguard Centre Den Helder
SOLAS	Safety of Life at Sea (IMO Convention for the… 1974)	
ESA	Equivalent Security Arrangement	
DoS	Declaration of Security	
DGB	Directoraat Generaal Bereikbaarheid	Directorate-General for Mobility and Transport
KVNR	Koninklijke Vereniging van Nederlandse Reders	Royal Association of Netherlands Shipowners
GMDSS	Global Maritime Distress and Safety System	

IEC	International Electrotechnical Commission	
IACS	International Association of Classification Societies Ltd	
ITU	International Telecommunication Union	
STCW	Standards of Training, Certification and Watchkeeping	