Overview

Consolidated interpretations

of

Security Rules and Regulations

by

The Netherlands Shipping Inspectorate (NSI)

Version	Created by	Date Approved
1.0 t/m 1.9	B.O. Maltha	2004 –2007
2.0	B.O. Maltha	28 January 2009
2.1	J. Schot	19 May 2009

a) Introduction

In response to September 11, 2001 regulations have been developed within IMO, regarding Maritime Security. These regulations, of which the main part can be found in the "International Ship & Port facility Security (ISPS) Code", have entered into force on July 1, 2004 and apply to passenger ships, cargo ships of 500 gross tonnage and upwards and mobile offshore drilling units, engaged on international voyages, and Port facilities serving such ships. The regulations are integrated into the SOLAS convention and contain requirements regarding, equipment, training and a quality management system for Security. Ships will have to comply with these regulations: without a certificate it will not be allowed to participate in international shipping.

The EU has approved a regulation, which goes even further than the Security requirements developed by IMO. This EU regulation has taken effect as of July 1, 2004. As an EU member, The Netherlands has to comply with this regulation.

For further information, please visit our website and the websites of the Dutch directorate general of freight transport (DGTL), the EU, the IMO and the Royal Association of Dutch Ship owners (KVNR).

b) Supervision

The supervision of the Dutch flagged ships with regards to Security is attributed to the Netherlands Shipping Inspectorate (NSI).
For questions and information, you can contact Mr. J. Schot or Mr. B. van der Voort at NSI. You can reach them via the general number: +31-(0)70-4564500, or via e-mail: security.ds@ivw.nl.

c) Interpretations:

The ISPS code and other SOLAS amendments leave several issues up to the Administrations of member-states to decide. Furthermore some issues may not be entirely clear. In order to avoid confusion, NSI has compiled the following overview with interpretations of a number of these issues.

This list will be updated, if necessary, with new or revised points of view. Please check regularly for the latest version, via the website of NSI:
www.ivw.nl

To make things more clear and to align this document with NSI policy, apart from recent changes and additions, a new chapter has been added. The current chapters with security information are:
E: “For Your Information”
F: “Ministerial regulations” (ministeriële regelingen) for those matters which have already been formalised through other official documents,
G: “policy rules” (beleidsregels), and
H: “interpretations”

Since many companies refer in their internal publications to the numbering of the issues in this overview, we have chosen to retain the old numbering. Since we also have removed several numbers that have been outdated, we advise you to always check which chapter you are in and which subject you are looking for. If you still have any questions, you can contact either NSI or your RSO or the Royal Association of Netherlands Ship owners (KVNR).

d) List of used Abbreviations:

Abbreviation	Meaning
ISSC	International Ship Security Certificate
ISPS	International Ship & Port Facility Security Code
NSI	Netherlands Shipping Inspectorate (part of IVW)
IVW	Transport and Water Management Inspectorate
RSO	Recognized Security Organization
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	Departmental 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	Coast Guard Centre (Kustwacht Centrum) Den Helder
SOLAS	Safety of Life at Sea (IMO Convention for the… 1974)
ESA	Equivalent Security Arrangement
DoS	Declaration of Security

e) For Your Information: procedures and other information

Below issues give further information on procedures etcetera regarding the ISPS certification process.

Issue Nr.: **005**	Subject: **Identification of RSO Auditors**

RSO Auditors need to identify themselves when inspecting an SSP or when performing a verification on board as follows:

- Valid passport or drivers license
- Proof of employment (RSO ID-pass or a signed letter by employer)
- Proof of competence (conform IACS PR 10 (up to 1 July 2009, PR 25))

The latter 2 may be integrated into 1 document or ID-card.
In case of doubt regarding the identity or qualification of a person claiming to be an RSO-auditor, the ship can contact the relevant RSO.

Issue Nr.: **007**	Subject: **Application procedure ISSC**

- You can request an ISSC through the RSO of your choice
- The SSP will be inspected by the RSO
- The on board verification will be done by the RSO
- As of August 1, 2006 ISSC's and interim ISSC's are issued by the RSO

Issue Nr.: **010** (&39)	Subject : **Security level**

- Unless otherwise notified, all ships registered in the Netherlands, should operate at security level 1 (See also MSC Circular 1132)
- This security level is established by the minister of the Interior and Kingdom Relations (as per art 63 of the Ships Act)
- The Coast Guard Coordination Centre (KWC) at Den Helder will communicate changes in security level of ships registered in the Netherlands to the relevant companies (preferably via CSO's). They should then inform their ship(s) as applicable and confirm to KWC that the change has been implemented on board.

Issue Nr.: **027**	Subject **KVNR Framework for Ship Security Plans (SSP)**

Using this guideline for drawing up the SSA and SSP does not guarantee issuance of an ISSC.

Issue Nr.: 33	Subject: Using the **Declaration of Security (DOS)**

- See IMO (MSC) Guidance, especially MSC circular 1132.
- See for retention time of the DOS issue nr 19 in chapter f: Ministerial Regulations

Issue Nr.: **035**	Subject: **Deficiencies at verifications by RSO's**

When deficiencies are found during verification, the following procedure shall be adhered to:

- RSO informs NSI according to Class Agreement (art 4.5)
- CSO and/or SSO shall take temporary alternative measures to maintain the required level of security.
- The alternative measures shall be approved by the RSO
- CSO and/ or SSO shall draw up action plan and time schedule to correct the deficiencies
- The action plan shall be approved by the RSO
- The CSO is ultimately responsible for the procedure

If the company does not abide by the action plan or time schedule without preceding consultation and agreement by the RSO, the ISSC may be withdrawn. As per August 1, 2006 the RSO is authorised to withdraw the ISSC. The RSO reports to NSI.

Issue Nr.: 037	Subject: Residence **of the CSO**

It is permitted for a CSO to reside outside the Netherlands.

Nr.: 048	Subject: **Application procedure Continuous Synopsis Record (CSR)**

a. The CSR application form is available through the website of the Transport and Water Management Inspectorate (IVW): www.ivw.nl
b. The application form can be completed in writing or digitally and shall be forwarded to IVW
c. This form can also be used when the registry with the Netherlands ceases
d. IVW shall issue the CSR's in the format as decided by the IMO
e. A CSR may only be issued if an ISSC has also been issued for the same ship
f. The original CSR-file shall be kept on board as long as the ship is in service
g. When a ship changes its registration to the Netherlands, and the previous flag state does not timely send the required documents, NSI shall issue a new CSR according to the instructions of IMO MSC resolution 198(80). This resolution adopts amendments to paragraph 8 and 9 of the annex to the existing IMO A Resolution A 959(23).

Nr.: 049	Subject: **Ships registered in the Netherlands Antilles or Aruba**

Please contact the Shipping Authorities in the Netherlands Antilles or Aruba (see http://www.ivw.nl/english/topics/merchant%5Fshipping/flagstate/security/contact%5Fdetails%5Fship%5Fsecurity/

Issue Nr.: **055 (and 036)**	Subject: **Certification and the SSAS**

- Each SOLAS ship registered in the Netherlands must have an operational and approved Ship Security Alert System (SSAS)
- The Company is responsible for this. This entails, amongst others, timely reporting the installation of the SSAS in newly built ships, for appropriate verification
- If the SSAS is not installed and approved, the ISSC may be revoked

- Relevant documents, describing the requirements for the SSAS, include:
  - ISPS Code
  - SOLAS XI-2, regulation 6
  - IMO resolution MSC 136(76) and MSC 147(77)
  - MSC Circulars 1072 and 1111 (MSC Circular 1073 can also be of interest)
- If any uncertainty or inconsistency exists regarding applicability of MSC Resolution 147(77) (Revised Recommendation on Performance Standards for a SSAS) and MSC Circular 1072 (Guidance on Provision of the SSAS), the latter prevails

NL Approach:

- The SSAS shall not be type approved or case approved by NSI
- At initial installation of the SSAS, this must be approved as per IACS Procedural Requirement nr 24 rev5, par 2.24, 4.5, 7.1, 7.4, 7.8 and 7.9, and IACS Unified Interpretation SC 194, taking into account the following guidelines:
- Regarding the Technical Approval:
  - If in newly built ships, immediate survey is not possible for a SSAS connected to the GMDSS, then it has to be disconnected from the GMDSS, until the survey can take place
  - The radio surveyor shall not access the SSP, but limit the survey to the hardware
  - All SSAS equipment must comply with the IEC 60945 norm and the relevant ITU specifications with regards to radio communication
- During any survey of the SSAS, the SSO, or a qualified and authorised substitute, shall be present, to explain the operation of the SSAS
- An RSO or Radio Technician may also request the attendance of a competent person in conjunction with the maintenance of SSAS, during a survey of the SSAS
- The CSO is responsible for timely informing all recipients of test messages (including the Coast Guard Centre) and the appropriate confirmation of test message receipt
- If it is established that the SSAS does not comply with the requirements
  - RSO shall report this to NSI immediately
  - The Company shall contact NSI as soon as possible, to solve this problem
  - During a radio survey: The safety certificate (VC) will be endorsed if the GMDSS itself functions as required
- If an SSAS is found operational, which is not tested as described above:
  - If Self Contained: The SSO has to test the system on the spot and log a report thereof. Also it must be proven that the SSAS equipment complies with the IEC 60945 norm and relevant ITU specifications with regards to radio communication
  - If attached to the GMDSS: An Approved Radio Technician has to test the SSAS and log a report thereof, before the RSO audit can be finalised.

Issue Nr.: **057**	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 for existing ships with a gross tonnage < 500 ton, have **NOT** been exempt from the requirement of having an ISSC
- The tonnage criterion to decide whether a ship should comply with the ISPS code is the

(new) GT measurement
- The IMO interim scheme (as per MSC circular 1157) has ceased as per July 1, 2008.

Issue Nr.: **059** Subject: **Contactdetails CSO for Changes in security Level**

To be able at all times to reach the Dutch fleet with regards to a change in the security level, other threat warnings or further instructions regarding security, it is imperative that the Dutch Government has a complete overview of all relevant CSO's and their contact details. The following data are required:

- Name CSO
- Office Telephone nr CSO
- Mobile Telephone nr CSO (24 hours)
- Home Telephone nr CSO
- E-mail address CSO
- Name and address of Company
- Telephone nr Company
- Fax nr Company
- Other relevant particulars (e.g. Alternative CSO)
- Name of relevant ship(s)
- Call sign of relevant ship(s)
- IMO number of relevant ship(s)

For many ships, these data have been sent to the Coast Guard Centre (KWC) in the past. As of January 1, 2006, the Inspectorate for Transport and Water Management will administer these data. The Inspectorate will ensure availability of these data to the KWC.

PLEASE DO NOT FORGET TO NOTIFY THE INSPECTORATE OF CHANGES IN THESE DATA!
The data can be sent:

By mail: Inspectorate for Transport and Water Management
Attention of Toezichteenheid Zeevaart (NSI)
With mention of: "CSO data"
P.O. Box 8634
3009 AP Rotterdam
The Netherlands

Or by fax to number: +31-(0)70-456 4513
Or by e-mail to: csodata@ivw.nl

f) Ministerial regulations

Below issues have been formalised through ministerial regulations which have been published in the "Staatscourant" (State Gazette). On each subject, reference is made to the relevant ministerial regulation.

Issue Nr.: **004 (&046)**	Subject: **EU regulation and Interpretations**
Ships registered in the Netherlands must comply with EU regulation 725/2004 (**See also Art 31.2 of "Regeling Veiligheid Zeeschepen" as published in the "Staatscourant" of December 23rd, 2004, nr 248).** The final version of the regulation can be found via Easyrules at the NSI website: http://www.ivw.nl/onderwerpen/koopvaardij/vlaggenstaat/wet_en_regelgeving/ Interpretations by NSI of the regulations of the ISPS Code and other SOLAS amendments prevail over deviating interpretations by an NSI-recognized RSO (for application on Dutch ships). If a dispute between company and RSO cannot be solved, please contact NSI. The report of the RSO will be treated as advice to NSI.	

Issue Nr.: **014** (&15)	Subject : **Training Ship Security Officer (SSO**

Ref. "Regeling certificering scheepsbeveiligingsfunctionarissen (**Ship Security Officers, SSO's)"** of March 28th , 2008/Nr. HDJZ/SCH/2008-373, as published in the "Staatscourant" of April 3rd , 2008, nr. 65. English translation:

Article 2: Before a certificate of proficiency for an SSO can be issued, the following conditions must be met:

1. Applicant must comply with Regulation VI/5, para 1.1, of the Annex to the STCW-Treaty, and have successfully concluded a training compliant with section A-VI/5, para 1 to and including 4, of the STCW-Code, given by a training institute that is recognised by the Minister of Transport, Public Works and Water Management of the Netherlands.
2. As an exemption to the previous paragraph, the Inspector-general of the Inspectorate for Transport and Water Management can, until July 1st 2009, issue the certificate of proficiency for an SSO, if the applicant can prove in writing that:
    - A. He or she has completed an SSO training prior to January 1st 2008, and
    - B. He or she has performed an approved service as SSO of at least 6 months, in period of 3 years prior to the application, or
    - C. He or she has performed security duties that can be seen as equivalent to those mentioned in para B above.

Article 3

1. Crew members that have been appointed as SSO must possess a valid certificate of proficiency as mentioned in Article 2
2. As an exemption to the previous paragraph, until July 1st 2009, crewmembers that have successfully completed SSO training prior to January 1st 2008, can be appointed as SSO.

RSO's will monitor this during on board verifications and during approvals of the Ship Security Plan, taking into account the requirements of the ISPS Code and relevant IMO Guidelines (a.o. MSC Circular 1097).

Application for the "Certificaat Scheepsbeveiligingsfunctionaris" (Ship Security Officer)

See the IVW website:
http://www.ivw.nl/onderwerpen/koopvaardij/bemanning/opleidingen/

Applications for certificates and training can be done with the training institutions mentioned on the website.

Issue Nr. : **019** (&20 &51)	Subject **Keeping of Records and DoS**

All records as specified in paragraph 10.1 of Annex 2 of EU regulation 725/2004 (part A of the ISPS code), shall be kept on board for a minimum period of 3 years.
See also Art 31.3 of "Regeling Veiligheid Zeeschepen" as published in the "Staatscourant" of December 23rd, 2004, nr 248

Storage period for DoS
Declarations of Security (DoS), which have been made in the timeframe within which the last 10 calls at port facilities have taken place, must be kept on board during this timeframe, with a minimum of 3 months.
See also MSC circular 1132 (ao par 17)
See also Art 31.3 of "Regeling Veiligheid Zeeschepen" after the changes as published in the "Staatscourant" of February 21, 2006, nr. 37, page 18

Issue Nr.: **031 (& 40)**	Subject **Ship Security alerts**

The Ship Security Alert for ships registered in the **Netherlands** must be transmitted (possibly via the CSO), to the Coast Guard Centre of the Netherlands (KWC) in Den Helder, currently ONLY via one of the following means:

- Via Fax at number +31 (0)223 - 658 358 (24/7), **OR**
- Via Telex at number 71088 KUSTW NL (24/7)

KWC cannot guarantee fast and efficient follow up of Ship Security Alerts that are received via E-mail.
Ref. Art 31.1 of "Regeling Veiligheid Zeeschepen" as published in the "Staatscourant" of December 23rd, 2004, nr 248, and "Communicatiehandleiding Security zeehavens en zeescheepvaart" issued by DGG

Ships registered in the Netherlands Antilles or Aruba
Alerts sent from ships registered in the **Netherlands Antilles or Aruba** shall be transmitted to the Coast Guard Centre at Curaçao, Netherlands Antilles. For further guidance in this matter, please contact the authorities responsible for Maritime Security in the Netherlands Antilles or Aruba.
See art. 22.1 of the "Regeling Antilliaanse en Arubaanse schepen" of December 16th 2004.

Sending alerts if the SSAS is temporarily out of order:
In this case, ships registered in the **Netherlands** can send Security Alerts via the following procedure:

- Ship informs the Company/ CSO (possibly via Dirkzwager)
- Company/ CSO (possibly via Dirkzwager) will contact the Departmental Coordination Centre for Crisis Management (DCC) of the Ministry of Transport, Public Works and Water

Management

- **Phone numbers of the DCC**:

General nr: **+31 (0)70 351 8555**
Emergency number**: +31 (0)800 322 8369**

National Point of Contact
See explanation of **Art 31 of "Regeling Veiligheid Zeeschepen" as published in the "Staatscourant" of December 23rd, 2004, nr 248:**
The Coast Guard Centre at Den Helder has been appointed as "*National point of contact*"

Issue Nr. : **052**	Subject: **Recognised Security Organisations (RSO's)**

With the Class Agreement of August 1st 2006, the following organisations have been authorised by the minister of Transport, Public Works and Water Management of the Netherlands to perform on board verifications and plan approval for the International Ship Security Certificate for ships registered in the Netherlands:

- American Bureau of Shipping (ABS)
- Bureau Veritas (BV)
- Det Norske Veritas (DNV)
- Germanischer Lloyd (GL)
- Lloyds Register (LR)
- Nippon Kaiji Kyokai (ClassNK)
- Registro Italiano Navale (RINA)

See "the Class Agreement of August 1st 2006

g) Policy Rules Merchant Shipping ("Beleidsregel Zeevaart")

The below interpretations have been formalised as policy rules ("beleidsregels"), as published in the "Staatscourant" on August 18, 2008, nr. 158.

Issue Nr.: **013**	Subject: **Changes to approved SSP's and security equipment**
Ref. article 2.3 of the policy rules Merchant Shipping ("Beleidsregel Zeevaart"). Changes to approved SSP's or security equipment, which affect the security performance on board, shall be reported to the RSO, before their implementation. The RSO decides in each case if the change is permitted and if verification will be necessary, based on guidance issued by NSI. (See Guidance document at NSI website: http://www.ivw.nl/english/topics/merchant%5Fshipping/flagstate/security/interpretations%5Fand%5Fprocedures/	

Issue Nr.: **15**	Subject: **Company Security Officer (CSO)**
Ref. Article 2.4 of the policy rules Merchant Shipping ("Beleidsregel Zeevaart"). CSO's must have the necessary knowledge, understanding and proficiencies to be able to properly perform the tasks and responsibilities assigned to them in Article 11 of part A of the ISPS Code (ref ISPS Code part A, article 13.1). Therefore a CSO must be able to prove that he has successfully concluded training compliant with art. 13.1 of part B of the ISPS code	

Issue Nr. : **030**	Subject **Internal reviews/audits of SSP**
Ref. Article 2.5 of the policy rules Merchant Shipping ("Beleidsregel Zeevaart"). • The minimal frequency, at which internal reviews/audits of each SSP shall be held, is at least once before intermediate or renewal verification takes place. • If drills or other experiences give cause to change the SSP, this shall be done as soon as possible, according to the existing procedure for changes to approved SSP's (issue 13) • Any actions and measures by companies, aimed at improving the observance and security awareness onboard their ships, are encouraged by NSI. The yearly performance of internal audits by the company (CSO) can be of assistance in this respect. Possibly, the Self Assessment Questionnaire as developed by the IMO and the EU, can be a useful tool for these audits.	

Issue Nr.: 034	Subject: **Frequency of searches of embarking persons**
Ref. Article 2.7 of the policy rules Merchant Shipping ("Beleidsregel Zeevaart"). To comply with article 9.4.1, of part A of the ISPS Code, and article 9.15 of part B of the ISPS Code the following minimal frequencies of searches have been approved by NSI, notwithstanding the obligations of the master as per Solas chapter XI-2, regulation 8.2: At security level: **1)** As deemed necessary by the SSO or CSO. The choice of frequency by SSO or CSO can either be documented per port call in the security logbook, or as a generic value in the SSP.	

2) 1 person out of 10 at random, with a minimum of 1 actual search per port of call **3)** All persons

Nr. : 041 Subject: **Certificates when registering existing ships in the Netherlands**
Ref. Article 2.1 of the policy rules Merchant Shipping ("Beleidsregel Zeevaart"). If the company remains the same, the procedure will be as follows: ▪ The SSP must be approved by an NSI appointed RSO, taking into account the specific Dutch regulations, policy rules and interpretations ▪ If an RSO has recently approved an SSP on behalf of an other flag state, this RSO could, in principle, suffice with only a check on the specific Dutch regulations, policy rules and interpretations ▪ An on board verification must be held according to the instructions issued by NSI. In principle this can consist of an earlier verification for another flag AND an extra verification limited to the specific Dutch regulations, policy rules and interpretations. If the above procedure is followed correctly, a long term ISSC can be issued. This applies to ships flagging in, with or without an ISSC from another flag state. If a new company takes control of the ship: ▪ A CSO must be appointed by the new company ▪ This CSO is responsible for all ISPS matters, including the performance of a new Security Assessment and the creation of a new SSP. If applicable, parts of the former SSP may be reused. This does not guarantee that the SSP will be approved. ▪ Basically the complete regular ISSC procedure must be followed. If, due to lack of time, problems might arise regarding the issuance of an ISSC, the company can request an interim ISSC. If the demands as stated in article 19.4.2 of part A of the ISPS code are met, an interim ISSC can be issued by the RSO, based on article 19.4.1 of part A of the ISPS code, referring to the transfer of flag. This will allow the relevant company a maximum of 6 months to qualify for the regular ISSC.

Nr. : 042 Subject: **Certificates for ships newly delivered**
Ref. Article 2.2 of the policy rules Merchant Shipping ("Beleidsregel Zeevaart"). Basically the complete regular ISSC procedure must be followed. If, due to lack of time, problems might arise regarding the issuance of an ISSC, the company can request an interim ISSC. If the demands as stated in article 19.4.2 of part A of the ISPS code are met, an interim ISSC can be issued by the RSO, based on article 19.4.1 of part A of the ISPS code, referring to the delivery. This will allow the relevant company a maximum of 6 months to qualify for the regular ISSC.

Nr. : 056	Subject: **Access Control**

Ref. Article 2.6 of the policy rules Merchant Shipping ("Beleidsregel Zeevaart").

- A**ccess control** is required under SOLAS security regulations (ISPS A 7.2.2)
- However, the ISPS code does not state that a **gangway watch** is mandatory

The agreement for the ships registered in the Netherlands is that there **needs to be access control**, but **not necessarily by a gangway watch**. For example, access control may be done by a man on deck or on the bridge, or via camera's, as long as someone is monitoring access to the ship and visitors are approached upon boarding the ship to enquire after the purpose of their visit. If these or similar forms of access control are not present, then the ship is not compliant.

The SSP should reflect the above and an RSO appointed by the Dutch government should only approve plans that conform to the above. If an RSO has approved plans that are not compliant with the ISPS code, this situation should be corrected immediately.

Some countries have established national or local laws with more strict demands for access control. CSO's and SSO's should take this into account when preparing voyages

Nr. : 058	Subject: **Shore based Contact point for follow up of SSAS alerts for ships where the CSO is also the master**

Only relevant for companies where the CSO is based on board the ship!!

Ref. Article 2.8 of the policy rules Merchant Shipping ("Beleidsregel Zeevaart").

- If the Coast Guard Centre (KWC) receives an alert via the Ship Security Alert System (SSAS), it will inform the Departmental Crisis Coordination Centre (DCC). The CSO will be contacted to gain relevant information and to check if there may have been a false alert. If the CSO is also the master on board of the ship concerned, this is not possible as authorities are not supposed to contact the ship directly after receipt of an SSAS alert (MSC Circular 1073, a.o. in art 2.4.2 of the Annex, regarding "Covert Alert").
- **To be able to appropriately respond to SSAS alerts of ships where the CSO is also the master**, there is a need for a shore based contact point.
- This can be the contact point as required by the registration laws and regulations, but also a third party (company 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 case of a security alert. The contact point must be able to supply as much relevant information as possible regarding the ship involved, such as type of ship, cargo, position, crew, presence of dangerous goods etc, to the Dutch government.
- The shore based contact point will be mandatory as per the date that the SSAS becomes mandatory
- Contact details of the shore based contact point must be reported to the Inspectorate for Transport and Water Management for all relevant ships, together with the CSO data
- For ships without a shore based contact point, the Dutch Government will assume that each SSAS-alert is a real emergency, and respond to the alert on that basis. It is therefore likely that inappropriate use of the SSAS will result in significant costs.

Nr. : 060	**Subject: Drills and Exercises**

Ref. Article 2.8 of the policy rules Merchant Shipping ("Beleidsregel Zeevaart").

Drills:
- Are to be performed by the ship, as required by ISPS part A para 13.4 and part B para 13.6. The SSO is first line responsible for the execution of these drills.

Exercises:
- ISPS exercises are different from drills, and have to be carried out, as per the requirements of ISPS part A para 13.5 and part B para 13.7, once a year with no more than 18 months between them
- The organisation is in principle company business (CSO), in line with the ISM system
- The purpose is to test the security-system of the company and to ensure the effective coordination and implementation of SSP's
- More than one company ship (if possible) but not all company ships have to be involved in a specific exercise
- However reports have to be sent to all company ships and the records have to be kept on board of all company ships
- Furthermore, necessary improvements identified through the exercise should be effectuated on all company ships registered in the Netherlands
- Authorities may be involved in these exercises but are not obliged to participate. Nevertheless authorities are encouraged to carry out their own exercises
- A CSO may participate in these governmental exercises and is in that case not obliged to organise a company exercise that year (ISPS part B, para 13.8). However in these cases reports do have to be sent and recorded in a similar way as with company exercises
- If a ship, when asked, is not able to provide its RSO or administration (at intermediate or renewal audits) with records of required exercises, the ISSC may be revoked

If a ship, when asked, is not able to provide Port State Control (PSC) officers with records of required drills and exercises, this may count as a security deficiency for the relevant PSC organization.

h) Interpretations

Issue Nr.: 038	Subject: Interpretations and their application
• Ships in possession of an approved SSP, have to establish adjustments to the SSP and/or the ship, which are necessary due to interpretations that were published after their SSP was approved, at the next intermediate or renewal verification. • An exception to this rule can exist, when NSI specifically mentions that the adjustments must be made immediately.	

Issue Nr. : 061 (see also issue 33) Subject: Use of the Declaration of Security (DOS) by a ship (ref part B5/A5: ISPS-code and IMO's MSC/Circ.1132):

General DoS

A ship has to comply with a request from a port facility to complete a DoS. However a port facility does not have to comply with a request for the completion of a DoS from a ship. It only has to acknowledge the ships request. Likewise a ship does not have to comply with a request for completion of a DoS from another ship, it only has to acknowledge the receipt of the request.

Generally, a DOS should only be established if there is a sound, security related reason to do so, at a specific ship/port or ship/ship interface. Situations in which it is advised to establish a DOS can be:

- Situations as described in article 5.2 of part A of the ISPS Code*
- Situations that are not covered by the SSP and/or the PFSP
- In case of ship/ship contact with a non-ISPS vessel carrying Dangerous Goods

Contact between ISPS ship and inland Barges

Specifically for dealing with barges carrying stores, bunkers, disposal of waste, etc, a DoS is not required as long as:

- The bunkering barge has an ISSC, or
- The barge is covered by the Port Facility Security Plan (PFSP)
- The SSP contains provisions for physical security measures for dealing with these barges, and these physical security measures are in place when the interface with the barges takes place, eg monitoring the barge, escorting the barge personnel

NSI recommends recording in the security logbook, that the appropriate security measures have been carried out.

The same principals apply to the loading /unloading to/from barges.

If a Dos is required and there is no one willing or able to sign the DoS from the inland barge, the ship shall fill in a DoS unilaterally AND RECORD ITS ADDITIONAL MEASURES TAKEN, as they may have to produce them in one of the next ports.

* According to section A/5.2 of the ISPS Code, it is specified that a ship can request a DoS when:

- The ship is operating at a higher security level than the port facility or ship it is interfacing with;
- There is an agreement on a DoS between Contracting Government covering international voyages or specific ships on those voyages;
- There has been a security threat or a security incident involving the ship or the port facility, as applicable;
- The ship is at a port which is not required to have implemented an approved Port Facility Security Plan; *or*
- The ship is conducting a ship-to-ship activity with another ship not required to have implemented an approved Ship Security Plan.