Sjøfartsdirektoratet
Norwegian Maritime Authority

Instructions to RSO

Category:		Instruction no.: 6/2017
□ Operational	□ Nautical	Our ref. and file no.: 2017/101278
□ Technical	☒ Other	Date: 13/12-2017
Authorized by: Alf Tore Sørheim		Signature: Olav Akselsen

Interpretations and requirements related to Security Rules and Regulations

Purpose

IMO developed chapter XI-2 of SOLAS and the ISPS code in order to deal with security related matters. EC later approved Regulation (EC) Nr. 725/2004 which goes even further than the requirements given by IMO. These international requirements leaves several issues to the Administration to decide. Norway have through Regulation 972/2004 implemented the international requirements.

This instruction to RSO is developed in order to clarify some of the Norwegian requirements, and to give the RSOs clear instructions concerning specific cases and interpretations.

Application

These instructions is valid for all processes related to issuance of an ISSC to a Norwegian flagged vessel.

Vessels that through their trade certificates are able to operate internationally, and otherwise falls within the scope of SOLAS are required to comply with the ISPS requirements.

It must be noted that SOLAS Chapter IX-2 and part A of the ISPS Code have no provisions for granting of exemptions.

1 SSP and SSA content and approvals

1.1 Mandatory parts from the B part of the ISPS code

Through EC and national regulations, some chapters in the ISPS code part B has been made mandatory for all Norwegian flagged vessels. That includes:
B.1.12, 4.1, 4.4-4.5, 4.8, 4.18, 4.24, 4.28, 4.41, 4.45, 6.1, 8.3-8.10, 9.2, 9.4, 13.6, 13.7

1.2 Working language and language used in SSP

It is required that the Company develops the SSP in the working language, as defined on board. If the working language is not defined to be English, it is required that the Company develops an English translation of the SSP as well. Both plans must stamped and approved by the RSO. Record of activities addressed in the SSP shall be in the working language of the vessel, if the working language is not English then a translation to English shall be provided and maintained.

1.3 Revisions done to the SSP

NMA accepts that Companies keep their SSP updated with relevant information (CSO changes, additional and improved security measures etc) without the need for re-approval of the plan. Changes to the plan must be able to be documented and only changes that does not reduce the security for the vessels, such as minor changes in ship data and arrangements that does not interfer with security related issues, minor organisatorial changes, CSO, SSO change, may be done without the need for re-approval. RSO shall verify and approve such revisions during the first planned verification on board.

1.4 Criteria for approving SSP and SSA

SSA and SSP should be submitted in a safe manner to the RSO. When sent by mail from Norway to Norwegian address, it is sufficient to submit it in a sealed envelope delivered by courier. When submitting it to/from another EC/EEA country, it must be inside a sealed envelope packed in another envelope, or sent by personal courier. SSA and SSPs that is to be sent outside Europe can be sent electronical in password secured shipment. SSA and SSP is not to be sent in the same shipment and shall be sent separately.

In any case, electronical shipment can be used as described above, also within Norway and EU/EEA.

SSA and SSP defines amongst others vessel types, trading area and cargoes carried. Changes to these parts of the SSP/SSA are considered to affect the content and analysis which the SSP is based on substantially, and therefore it is necessary to re-approve the SSP.

A qualified individual, taking into account all available information from relevant authorities and other resources, must develop SSA. Other resources used shall be documented in the SSA.

NMA accepts electronic versions of the SSP, as long as they fulfil the requirements with documented revision history etc. The vessel shall in those instances have the following pages stamped and signed by RSO available on board: SSP front page, SSP Index and SSP amendments page.

SSA may not be developed by the RSO, if the same RSO are to approve the SSP.

1.5 SSAS

NMA requires that SSAS testing to be done on a regular basis. From our view it would be sufficient if such tests are performed at 6 month intervals. At least one of the test shall include the national contact point (JRCC-Sola).

SSAS should be programmed to send alerts to: ssas@rescue-norway.org

1.6 Access Control

It is required that persons seeking to board a vessel should not be able to do that unchallenged. Open gangways, gangways with information posters, gangways with rope and informational posters are not considered to be a challenge for persons seeking entry to the vessel by NMA. SSP must include instruction as to how the vessel is controlling persons seeking access to the vessel and ensuring that they able to identify themselves and their purpose with the visit to the vessel before they have gained access to the vessel.

Vessels that are going to perform, or are likely to perform, “double banking” shall have written instructions on how to proceed with such operations and at the same time remain in control of the security measures implemented in order to ensure that people seeking access to own vessel are being controlled.

1.7 Frequency of searches

ISPS code defines that the SSA should identify the frequency of visitor, baggage and cargo. On security level 1, SSP must identify a higher value than 0%. In order to demonstrate that these requirements are met, vessel must be presented with guidance on how to document such searches, and what to look for.

For security level 2 the searches must be done on at least one person/item if cargo/storage/persons taken on board is higher than on security level 1.

1.8 Drills and exercises

Drills: To be performed by the vessel as required by ISPS Code A13.4 and B13.6

Exercises: To be performed once a year, and not exceeding 18 months between two of them. To be performed as described in ISPS Code A13.5 and B13.7. The main purpose is to do a full test of the security system, and to ensure effective coordination and implementation of the SSP. One or more vessels in a company’s fleet may participate, but all vessels must be able to take part of the summary and experience transfer reports after such exercises. Authorities may participate in such exercises, but are not obliged to participate. If a company or operator have vessels registered in different flag state, reports and evaluation reports from exercises conducted on vessels can be used as documentation for executed exercises as long as they are in compliance with regulation given in relevant legislation.

1.9 Access to the approved SSP

The SSP should clearly state the criteria for how and whom to give access to the SSP or parts of the SSP.

NMA have issued ID cards with picture, name and validity dates for all inspectors that should have unhindered access to the complete SSP on board a Norwegian flagged vessel. Inspectors with access to the SSP must have "ISPS Control" printed on the back side of that ID card.

Foreign authorities should only be granted access to some part of the SSP, based on their need and authorization, as described in ISPS Code A9.8.1.

The SSP should include procedures to ensure that content directly related to A9.4 subsection .2, .4, .5, .7, .15, .17 and .18 never are given to foreign flagged authorities without prior agreement with NMA.

1.10 DoS

The SSP should clearly outline that the DoS shall only be drawn up and kept as a part of the vessels records as long as there is a justified security related reason for doing so.

1.11 Evacuation procedures

ISPS Code requires that the approved SSP describe the evacuation procedures. NMA accepts that existing SMS procedures regarding evacuation are linked or in other ways are made available in the SSP. Revisions to this SMS procedure will therefore also be a part of the verification and requirements described under 1.2.

1.12 Relevant contact points and responsibilities

NMA have published an updated list of relevant contact points, and their responsibilities according to EC Requirements on our homepage: www.sjofartsdir.no/isps

2 Verifications on board

2.1 Deficiencies identified on board

ISPS code does not include any possibilities for vessels to sail with open deficiencies. NMA requires anyone performing verifications (interim, initial, intermediate, additional and/or renewal) on behalf of Norway to ensure that acceptable measures are implemented, if deficiencies are observed during a verification.

The non-conformity shall be listed in the verification report for the Company to further address, together with a summary of the accepted measures implemented. Deficiencies and non-fulfilment of specified requirements (SSP, regulations etc) shall under no circumstances be listed as observations as they are clearly a deficiency/non-conformity.

Certificates may not be issued or endorsed on board a vessel with non-conformities that has not been rectified with a corrective action.

RSO shall notify the NMA of any ISPS-related deficiency found on NIS/NOR vessels, and without delay provide the NMA with a copy of the relevant verification report and accompanying corrective action plan. Furthermore, the RSO shall without delay provide the

NMA of confirmation when deficiencies are closed. When relevant, the confirmation on closed deficiencies shall include information on any equivalent measures effectuated for the audited vessel. If the vessel is not able to implement any corrective actions while the RSO is on board, the ISSC should be withdrawn. NMA is to be notified about any such actions.

2.2 SSAS

If an SSAS is not installed, approved, in working condition or alternative security measures approved by the flag are implemented when a verification is performed, the ISSC should be revoked.

2.3 Personal certificates

SSO: It is required that the SSO on board is holding a valid STCW VI/5 “Certificate of proficiency as SSO”. Diplomas and other types of documentation are not considered as valid proof of proficiency. The deadline to apply for a new “Certificate of proficiency as SSO” based on older courses ended in 2012. After this date, all SSOs should hold a STCW VI/5 “Certificate of proficiency as SSO”.

Crew: All crew with any tasks listed in the approved SSP shall hold STCW VI/6 “Certificate of proficiency for seafarers with designated security duties”.

Crew: All other crewmembers shall hold a STCW VI/6 “Certificate of proficiency in security awareness”.

2.4 Familiarization on board

All crewmembers on board shall have received security related familiarization training according to STCW requirements. The familiarization training shall be appropriate to the vessel they are employed on board, and being conducted by a qualified individual on board (SSO or another equally qualified person). Company must ensure that there are documentary evidence for the familiarization trainings completed, and that the person conducting these familiarization trainings are qualified.

2.5 Records

All records of activities addressed in the SSP shall be kept on board for at least the last 3 years (and for the last 10 ports of call if that time period exceeds 3 years).

All records shall be kept in the working language of the vessel, as defined in the SMS/deck logbook. If the working language is not English a translation into English shall be included on board.

2.6 DoS

A DoS is not mandatory when interacting with barges (bunkers, stores, waste etc) as long as the barge (when unloading/loading from barges):

- Is in possession of an ISSC

- Is covered by a Port Facility Security Plan

If vessel is interacting with ports, port facilities, platforms, MODUS, floating platforms and/or vessels without ISPS certification, a DoS shall be completed. A person responsible for the safety/security and/or operations on the interacting port facility/vessel may countersign the DoS.

2.7 Drills and exercises

The Company shall conduct an annual security exercise with one or more vessels within its fleet. All vessels in the fleet must receive a full report from the exercise and the lessons learnt from it, and keep that as a part of the drills/exercise records on board the vessel.

2.8 Access to the vessel

A person upon arrival to the vessel shall control all persons seeking access to the vessel, in order to verify their business on board.

Public authorities, such as police officers and custom control shall have immediate access to the vessel when bearing uniform. Signature in visitor log can be carried out when leaving the vessel. Public authorities not wearing uniform shall follow the instructions related to stated procedures in SSP regarding access control.

NMA inspectors seeking access to a vessel will have NMA issued ID cards. The validity of the ID card may be verified by calling our 24/7 telephone number: +47 52 74 50 00

2.9 Security level

The Contracting Government have authorization to raise/lower security levels. The Master/SSO may when he finds it needed implement the measures described in the SSP, but never officially raise the security level by himself on board the vessel and document a security raise in the records. Implementation of additional security measures from the SSP should only be recorded in the deck log book.

3 Certificates, verifications, change of RSO and Lay-Up

3.1 Interim certificate

An interim certificate can only be issued for a total of 6 months. NMA does not accept extensions to the interim certificates and/or the use of consecutive certificates. For those exceptional circumstances where it according to the requirements could be possible to extend validity of the interim certificate, acceptance from NMA must be granted before the certificate is updated.

3.2 Full term certificates

NMA requires full term certificates to be issued for a maximum of 5 years validity from the date of the initial verification.

3.3 Intermediate verifications

Intermediate verification to be carried out according to IACS guidelines.

3.4 Additional verifications

ISPS code defines that additional verifications shall be performed as determined by the Administration. NMA have defined the following criteria for when an additional verification shall be performed by RSO on behalf of the flag:

- As a follow up on port state control/detentions
- Follow up on sub-standard audit results (after corrective actions already being implemented)

The scope for such verifications should be based on the findings and root causes of these from the port state/detention and/or audit results.

NMA to be informed on email about all additional verifications carried out on Norwegian flagged vessels.

3.5 Changing to Norwegian flag

Changes between the two Norwegian registers (NOR/NIS) is not considered to be a change of flag.

NMA does not accept SSP and SSA developed for other flags without being re-approved based on Norwegian specific requirements, followed by new verification(s) on board.

ISPS A19.3.8.4 states that the ISSC (and the SSP) cease to be valid when transferring to new flag. Therefore it will be required to submit a new SSA and SSP based on Norwegian requirements for approval, and then have verifications held on board after flag change.

If an RSO previously approved the SSP on behalf of another flag state, this RSO could in principle, after a new approval of SSP under Norwegian flag, go directly for the initial verification on board. NMA to be consulted in such cases.

3.6 Changes in trade areas, company etc

Changes in trade areas, change of owners/company etc, may be considered to be major changes to the security of the vessel. SSP is developed based on assessments and vulnerabilities identified in the SSA. Any changes to those conditions will result in an invalidation of the SSP.

NMA to be consulted in those instances where it could be reasoned that those changes is of no implications for the already approved plan.

3.7 Change of RSO

NMA accepts that an already approved SSP under Norwegian flag is transferred to another RSO approved by NMA. IACS guidelines for such transfers to be followed.

3.8 Lay-up

With regard to the security of laid-up ships, it is a precondition that the ship has been satisfactorily secured against unauthorised access. This means that the ship shall have a watch keeping arrangement that ensures that unauthorised persons cannot gain access on board, and that any visitors are logged with time and duration of visit.

1. Consequences for ISSC:
   Lay-up period of up to 3 months: No consequences apart from the requirement to do a thorough search of the ship prior to departure in order to uncover any irregular conditions on board. The ship may then sail with its original ISSC.
2. Lay-up period from 3 to 6 months: In addition to the action mentioned in point 1, a physical verification audit shall be carried out on board the ship, either by the NMA or an RSO (Recognized Security Organization). The purpose of the verification is to confirm that any changes made on board during the lay-up period are not in conflict with the ship's security plan, and that technical equipment included in safety measures are found on board and are in working order.
3. Lay-up period of more than 6 months: The ship must be subjected to a new interim certification pursuant to the current regulations unless exceptional circumstances indicate that an exemption should be granted. Exemptions may be granted following a written application to the NMA.

3.9 Extension, suspension, withdrawal an reinstatement of certificates

If an ISPS verification is overdue, the ISSC is considered invalid. Company would need to start a new certification process in order to obtain a valid ISSC again. NMA accepts Companies to request initial verifications directly, if their previous certificate was a full term one.

NMA shall be notified about all ISPS verifications that becomes overdue, in order to withdraw/invalidate the ISSC, and to evaluate if RSO should be instructed to perform an additional DOC audit.

4 Auditors/inspectors and others involved in ISPS related matters for Norwegian flagged vessels

4.1 Qualifications

All personnel directly involved in verifications shall be able to document that they are qualified for that type of work, including the requirement to maintain and improve the expertise within maritime security.

RSO must ensure that the trustworthiness of their inspectors are regularly verified.

5 Reporting

RSO shall once a year send an updated list of all vessels in their portfolio with relevant security details. The report shall be submitted no later than the 31st of January. The list shall include at least the following details for all vessels:

1. Vessel name
2. IMO number
3. Company name (DOC holder)
4. Company IMO number
5. ISSC date of issue
6. RSO name
7. RSO regional/district/local office carried out the verification issued the ISSC
8. SSP approval date
9. Name of RSO approving the SSP
10. RSO regional/district/local office who approved the SSP
11. Number of deficiencies identified during last verification on board
12. Status and plans on deficiencies that is not rectified

NMA template for the report to be used,or data exchange with “Tilsynssystemet” to be set up in order to ensure regular update to our systems.

6 Audits and observations of RSO by NMA

RSO shall cooperate with NMA in the accomplishment of its auditing/observation tasks. The cooperation shall be effective during the preparatory, control and reporting phases. RSO shall ensure that NMA are able to exercise their authority to verify the Maritime Security activities as described EC No 725/2004.

7 Cases not covered in this circular

For all cases not clearly defined in the ISPS code, EC 725/2004 and/or Norwegian national regulation 972/2004, NMA to be consulted through the established communication lines for ISPS related matters.