17 March 2014

Human Environment and Transport Inspectorate
Ministry of Infrastructure and the Environment

Instruction to Recognised (Security) Organisation

No. 25 - Security related issues

Date entry into force: 03-04-2014

1 General introduction

The purpose of this instruction is to harmonize the application of ISPS Code legislation and interpretations by RSO's for vessels under Dutch flag.

2 Regulatory framework

Introduction
The regulatory framework consists of

- Class agreement dated 03 April 2014
- IACS Procedural requirement No. 24, as amended
- Consolidated Interpretations os Security Rules and Regulations by The Netherlands Shipping Inspectorate.

Rectifying and communicating non compliances
Major failures or major non conformities (as referred to in IACS Procedural requirement no. 24 (as amended) are considered as severe non compliances and when found during a verification are to be communicated to the Administration (NSI) immediately by e-mail or telephone (to be confirmed in writing).
A ship may decide to make up an ESA, conforming SOLAS Ch XI-2, Regulation 13:6 *Any Contracting Government which allows, under the provisions of regulation 12, any equivalent security arrangements with respect to a ship entitled to fly its flag or with respect to a port facility located within its territory, shall communicate to the Organization particulars thereof.* Such security measures are at least as effective as those prescribed in SOLAS Ch XI-2 or part A of the ISPS-code.
ESAs should not allow SOLAS ships to avoid full compliance with the requirements of the Maritime Security Measures. The Administration (NSI) reports an ESA to IMO (in GISIS).

3 Protection from unauthorized access or disclosure

Best Practices

Objects
The need to protect particular information (PI) must be considered on the contents of that information. It includes SSA, SSP, SSP amendments, and documents detailing measures put in place.

Staff

- For staff who have access to PI, conduct will be specified in procedures or job descriptions.
- Inspection of PI by authorized personnel only. Staff is screened before starting their duties and results are recorded. Annually, integrity is discussed during interviews.

Transport of information (physical and electronic)

- Transmission of PI (hard copy, CD-ROM, DVD, USB-stick or similar), by company or by RSO, preferably by courier or by registered post with tracking facility. Sender and receiver communicate time of dispatch and arrival of physical transport. Preparing for this shipment by authorized persons appointed in a neutral and sealed envelope.
- Companies may send PI in electronic format on a CD-ROM, DVD, USB-stick or similar. In case PI is forwarded through the e-mail it should be encrypted or password protected and passwords (if applicable) are to be sent separately via a different medium.
- If an RSO receives unencrypted PI by e-mail, they print it, save it on CD-ROM, DVD, USB-stick or similar and delete mails with PI from computers connected to the network. The sender will be requested to delete the e-mail with PI from their servers.
- Within own secure networks encryption is not required.

Physical security (buildings, workspace and cabinets)

- The building of a RSO has 24/7 access control at the individual level. Registration and identification of individuals.
- Room with PI is lockable, no access to a room with PI by third parties without accompaniment.
- No PI is left unattended by the auditor at the end of the day. All PI (hardcopy, (un)encrypted information) and stamps for official documents are stored in a lockable cupboard.

Information management

- Information carriers (CD-ROM, DVD, USB-stick or the like) are used so that the information cannot come to unauthorized persons (e.g. by using encryption).
- An auditor does not make more reproductions (hard copy and electronic) than necessary for review.
- After review no PI or reproductions may be kept (hardcopy or electronically) and they are to be deleted / shredded as appropriate.
- For archiving purposes the following information may be stored; front page, table of contents, page revision (with stamps).

Security breach

- The RSO will ensure NSI will be informed of security events and weaknesses related to information security. Events can be the unauthorized access, use or manipulation of information.
- The RSO is responsible for taking corrective action in time.