

**Minimum Requirements for Ship Security Assessments**

**1. Application of ISPS Code Part B**

- a. In general personnel involved in conducting Ship Security Assessments are encouraged to use the methodology and guidance set out in the United States Coast Guard (Navigation and Vessel Inspection Circular NVIC 10-2) which for the sake of completeness has been included in Appendix 3 of this Shipping Notice
- b. ISPS Code Part B Paragraphs 8.1 to 13.8 must be fully taken into account when conducting Ship Security Assessments (SSA) and developing Ship Security Plans (SSP). Not all paragraphs will be applicable to every ship. Where a paragraph is not considered applicable or suitable, the company submitting the SSA and SSP should be able to justify the paragraph's exclusion.
- c. Example: Paragraph B/9.40 calls for 100% x-ray screening of unaccompanied baggage at Security Level 3. This will be impractical for many ships to implement and so it would be acceptable not to implement these measures provided the ship does not to accept unaccompanied baggage onboard at this Security Level or if screening equivalent to the guidance given in B/9.40 is employed.

**2. Conducting Ship Security Assessments**

- a. Ship Security Assessments should be conducted by persons with appropriate skills to evaluate the security of a ship. As a general rule, those conducting SSAs should have completed a recognised Company Security Officers training course. Other qualifications and experience will be accepted on a case by case basis.
- b. Evidence of qualification of those conducting SSAs should be included with the SSA when it is submitted with the SSP.
- c. It is acceptable to follow standard methodologies<sup>2</sup> for conducting SSAs provided that all requirements for the SSA are addressed (See also "Application of ISPS Code Part B", above).

**3. Fleet Wide Ship Security Assessments**

- a. It is recognised that there will be similarities between both the threats present and the mitigation measures applied between ships operated by a single company. It is acceptable to conduct a "fleet wide" SSA, provided the individual characteristics of each ship is addressed (probably during the on-scene security survey and individual SSA Report).

**4. Threat Assessments**

- a. Threat assessments form an important part of conducting SSAs. Generally threats are categorised as a function of their likelihood to occur and the consequences should they occur. Although this is a mainly qualitative process, the SSA should contain sufficient justification to validate each decision reached.
- b. The threat assessment should be a *"systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual or function"* and

---

<sup>2</sup> Examples include those available from Classification Societies, Industry Groups, Administrations, etc

## Appendix 1: Ship Security Assessments

should *"identify actions to reduce the vulnerability and mitigate the consequences of a security breach"*. Threat assessments which consist solely of unsupported "tick boxes" will not be accepted.

### 5. On-scene Security Survey

- a. The on-scene security survey is an essential element of conducting any SSA. By definition, the on-scene security survey must be conducted onboard each ship.
- b. It is unlikely that any ship will have a valid reason for excluding the guidance given in ISPS B/8.6 (identified points of access to and within the ship) or ISPS B/8.14.1 - 7 (on-scene security survey) from the SSA.

### 6. Ship Security Assessment Report.

- a. The SSA must accompany the SSP for approval in the form of a written report which is to include:
  - i. A summary of how, when and by who the SSA was conducted.
  - ii. The findings of the on-scene security survey.
  - iii. A description of each vulnerability identified.
  - iv. Proposed countermeasures to be included in the SSP.
- b. The report should contain evidence that the assessment has been reviewed and accepted by the company.