



IMO

*E*

Ref. T2-MSS/2.11.1

MSC.1/Circ.1283  
22 December 2008

## DRAFT MSC CIRCULAR

### NON-MANDATORY GUIDELINES ON SECURITY ASPECTS OF THE OPERATION OF VESSELS WHICH DO NOT FALL WITHIN THE SCOPE OF SOLAS CHAPTER XI-2 AND THE ISPS CODE

1 The Maritime Safety Committee, at its eighty-first session (10 to 19 May 2006), recalling the request of the Tokyo Ministerial Conference on International Transport Security, held on 12 and 13 January 2006, for the Organization to undertake a study and make, as necessary, recommendations to enhance the security of ships other than those already covered by SOLAS chapter XI-2 and the ISPS Code, agreed that the development of recommendations aimed at enhancing the security of those ships would be desirable and would contribute to the efforts of the Organization to enhance maritime security and that such recommendations would need to be practical, sustainable and proportionate to the risks and threats involved.

2 The Committee, at its eighty-second session (29 November to 8 December 2006), began consideration of issues relating to the security aspects of the operation of vessels which do not fall within the scope of SOLAS chapter XI-2 and the ISPS Code (non-SOLAS vessels), and established a correspondence group on these issues.

3 The Committee, at its eighty-third session (3 to 12 October 2007), considered how to progress the issue of security aspects of the operation of non-SOLAS vessels and re-established a correspondence group on these issues and agreed the following categories of vessel to be covered by the Guidelines:

- .1 commercial non-passenger and special purpose vessels;
- .2 passenger vessels;
- .3 fishing vessels; and
- .4 pleasure craft.

4 The Committee, at its eighty-fifth session (26 November to 5 December 2008), approved the non-mandatory Guidelines on security aspects of the operation of ships which do not fall within the scope of SOLAS chapter XI-2 and the ISPS Code, as set out in the annex, as guidance for Member States.

5 This guidance is non-mandatory and has not been designed to form the basis of a mandatory instrument.

6 It has been formatted in two parts. Part 1 of the annex contains information of interest to Member States and other authorities with responsibility for administering non-SOLAS vessels (other authorities). Part 2 of the annex contains information pertinent to the owners, operators and users (operators) of non-SOLAS vessels and related facilities, with appendices containing information specific to the four vessels categories.

7 Member States are invited to consider these non-mandatory Guidelines and take action as appropriate.

\*\*\*

**ANNEX****GUIDELINES ON SECURITY ASPECTS OF THE OPERATION OF  
VESSELS WHICH DO NOT FALL WITHIN THE SCOPE OF  
SOLAS CHAPTER XI-2 AND THE ISPS CODE****Foreword**

These Guidelines are intended to provide information and best practice guidance to Member States and other authorities with responsibility for administering non-SOLAS vessels (other authorities), and operators of non-SOLAS vessels.

The Guidelines may be utilized by Member States and other authorities at their own discretion. They are non-mandatory and their application should be under the purview of individual Member States proportionate to assessed levels of threat and risk. The Guidelines are not intended to form the basis for a mandatory instrument. The Guidelines reiterate the importance of undertaking a risk assessment to determine if and to what extent such Guidelines are to be applicable.

The Guidelines have been formatted in two parts. The first part contains information of interest to Member States and other authorities with responsibility for administering non-SOLAS vessels (other authorities). The second part contains information pertinent to the operators of non-SOLAS vessels and related facilities, with appendices containing information specific to the four categories of vessels.

Member States and other authorities may wish to use the annex and its appendices to assist the operators of non-SOLAS vessels and related facilities to implement effective security. In doing so, Member States and other authorities are encouraged to promulgate appropriate contact information.

The Guidelines should not be interpreted or applied in a manner inconsistent with the proper respect of fundamental rights and freedoms as set out in international instruments, particularly those relating to maritime workers and refugees.

The Guidelines take into account the risk context for non-SOLAS vessels. Non-SOLAS vessels have been used for terrorist attacks and actions resulting in injury of innocent persons and destruction of ships and structures. They have also been used for smuggling operations.

## Contents

### Foreword

#### **Part 1: Information for Member States and other authorities with responsibility for administering non-SOLAS vessels (other authorities)**

1	Risk Assessment	3
2	Maintaining security awareness and reporting suspicious activity	3
3	Training and personnel practices	4
4	Non-SOLAS vessels on international voyages	4
5	Using available means of vessel identification (where appropriate)	4
6	International quality standards	6
7	Assisting operators of non-SOLAS vessels to understand practices for interacting with ISPS Code-compliant vessels and port facilities	6
8	ISPS Code as industry best practice for certain non-SOLAS vessels	6
Appendix	Risk Assessment and Management Tools	7

#### **Part 2: Information for use by owners, operators and users (operators) of non-SOLAS vessels and related facilities**

1	Risk assessment	19
2	Maintaining security awareness and reporting suspicious activity	19
3	Awareness of basic security requirements of SOLAS chapter XI-2 and the ISPS Code	19
4	Awareness of basic requirements for interacting with ISPS-compliant ships and port facilities	20
5	Training and personnel practices	21
6	Security measures	21
7	Planning for security events	24
Appendix A	Guidelines for commercial non-passenger vessels	28
Appendix B	Guidelines for non-SOLAS passenger vessels	30
Appendix C	Guidelines for fishing vessels	33
Appendix D	Guidelines for pleasure craft	35
Appendix E	Guidelines for marina, port and harbour authorities	38

## **Part 1: Information for Member States and other authorities with responsibility for administering non-SOLAS vessels (other authorities)**

### **1 Risk Assessment**

1.1 Member States and other authorities with responsibility for administering non-SOLAS vessels (other authorities) may wish to consider the risk context for each category of non-SOLAS vessel.<sup>1</sup>

1.2 A tool to assist Member States and other authorities with undertaking risk assessments is attached in the Appendix.

### **2 Maintaining security awareness and reporting suspicious activity**

2.1 Member States and other authorities may wish to encourage operators of non-SOLAS vessels to provide all personnel with information on how to reach appropriate officials and authorities in the event of security problems or if suspicious activity is observed. This information should include contact information for the officials responsible for emergency response, the national response centre(s) (if appropriate) and any authorities that may need to be notified.

2.2 Member States and other authorities may wish to engage with operators of non-SOLAS vessels and relevant organizations in developing security initiatives with respect to education, information sharing, coordination, and outreach programmes. Member States and other authorities may wish to consider establishing programmes to improve vessel operators' security awareness<sup>2</sup> and to promote links with the Administration's maritime security services.

2.3 Authorities responsible for establishing and maintaining security awareness and culture should be mindful of the need for the proper balance between the needs of security and the requirement to maintain the safe and working efficiency of vessels. These authorities should take into account the Human Element and the rights and welfare of seafarers and maritime workers, including the relevant provisions of the ISPS Code, when implementing these Guidelines.

---

<sup>1</sup> Examples of guidance and tools for undertaking a risk assessment of vessels may be found in:

- ILO/IMO Code of Practice on Security in Ports.
- MSC.1/Circ.1193: Guidance on voluntary self-assessment by Administrations and for ship security.
- American Bureau of Shipping: Ship Security Plan Review Checklist.
- United States Coast Guard Navigation and Vessel Inspection Circular 10-02: Security Guidelines for Vessels.
- Norwegian Shipowners' Association: Guideline for performing Ship Security Assessment.

<sup>2</sup> Two programmes are offered as models. In the United Kingdom, Project Kraken delivers an enhanced counter terrorist "vigilance" capability within the maritime environment of the Solent area on the South Coast. It engages key stakeholders together with local communities to provide a hostile environment to terrorists and criminals looking to disrupt the everyday lives and safety of those who live, work, or travel through the Solent. Project Kraken provides a single central phone number for the reporting of unusual activity or behaviour within the maritime environment that might be linked to criminal or terrorist acts. Similarly, in the United States, the *America's Waterway Watch* programme utilizes existing reporting systems within a public outreach programme, encouraging participants to report suspicious activity to the U.S. Coast Guard and/or other law enforcement agencies.

### **3 Training and personnel practices**

3.1 Member States and other authorities may wish to develop security policies and procedures, taking into consideration security assessments, to ensure that all operators and crew members (and passengers where appropriate) are familiar with basic security measures applicable to each of the vessel categories.

3.2 Basic security familiarization training is recommended for crew members enabling them to have the capability to respond to security threats. In higher-risk environments, this training should also have the purpose of testing and assessing competence and knowledge for effective implementation of the recommendatory security measures contained in these Guidelines.

3.3 Operator proficiency training for pleasure craft owners and operators could encompass security awareness familiarization.

### **4 Non-SOLAS vessels on international voyages**

4.1 Non-SOLAS vessels engaged in international voyages may be required to declare arrival and departure information for purposes of obtaining a port clearance from the relevant authorities. This declaration may be required within a specified period as determined by local authorities following arrival and/or prior to departure. The information to be submitted may include the particulars of vessel, date/time of arrival, position in port, particulars of Master/owner/shipping line/agent, purpose of call, amount of cargo on board, passenger and crew list, and emergency contact numbers. This declaration would enable the relevant authorities to better conduct monitoring and enforcement activities on the movement of vessels arriving/departing their port.<sup>3</sup>

4.2 Additionally pleasure craft or any other non-SOLAS vessel departing a port could be required to submit voyage information when applying for port clearance. The voyage information may include the estimated time of departure, destination and the planned route of the trip. The additional information may be useful to the relevant authorities not only in monitoring and enforcement activities, but also when conducting search and rescue operations should the vessel run into trouble and require assistance.

### **5 Using available means of vessel identification (where appropriate)**

5.1 The IMO vessel identification number is made of the three letters “IMO” followed by the seven-digit number assigned to all vessels by the Lloyd’s Register Fairplay when constructed. This is a unique seven-digit number that is assigned to propelled, seagoing merchant vessels of 100 gross tonnage and upwards and all cargo vessels of 300 gross tonnage and upwards upon keel laying with the exception of the following:

- Vessels solely engaged in fishing;
- Vessels without mechanical means of propulsion;
- Pleasure yachts;
- Vessels engaged on special service (e.g., light vessels, SAR vessels);
- Hopper barges;

---

<sup>3</sup> An example of such a programme is the declaration of information by pleasure craft currently required by Singapore via their Maritime and Port Authority Port Marine Circular No.17 of 2003.

- Hydrofoils, air cushion vehicles;
- Floating docks and structures classified in a similar manner; and
- Wooden vessels.

5.2 Member States and other authorities may wish to consider encouraging operators of pleasure craft to register with the Administration or a suitable organization which could provide a database available for authorized online access to assist in both preventative and response activities related to both safety and security.<sup>4,5</sup> It should be noted however that registration in itself offers no protection against the misuse of a registered pleasure craft which may be stolen, hijacked or even legally acquired.

5.3 Pleasure craft engaged in international voyages present unique circumstances. Even when registered, information regarding vessel characteristics, ownership, etc., is often not shared between countries of departure and arrival. This can result in a lack of transparency for security and safety organizations, leading to, for example, complications in validating an arriving vessels identity. Member States and other authorities may wish to seek agreements to provide for such information sharing, within the context of their individual laws and regulations, possibly as part of their individual coastal security initiatives.<sup>6</sup>

5.4 Member States and other authorities may consider (where appropriate) recommending the fitting of automated tracking equipment for ships which are not included in the requirements of SOLAS chapter V. The benefits of such a system could include:

- Enhanced safety and security;
- More rapid emergency response to maritime accidents and casualties;
- Better and more effective SAR capabilities;
- Better control of smuggling and human-trafficking attempts;
- Better control of illegal, unregulated and unreported fishing.

5.5 Such an automated tracking system could include the Automatic Identification System (AIS), Radio Frequency Identification Device (RFID) tags, Vessel Tracking Systems (VTS), and radar-based systems.

---

<sup>4</sup> Such a registration system may be seen in Finland, where all pleasure craft with a minimum length of 5.5 metres, or with an engine power of at least 15 kW, including sailboats, are required to be registered. The vessels are required to be visibly marked with a registration number, and registration documentation containing information regarding the owner, vessel and engine technical specifications and serial numbers is mandatory in order for the pleasure craft to be used. The register of information is kept by local city administrative courts and the registration number can be traced to the appropriate register.

<sup>5</sup> Another example may be found in the United Kingdom, where the authorities have created the United Kingdom Small Ships Register (SSR). This is simpler and cheaper than full vessel registration and specifically aimed at pleasure craft. Owners benefit by having details of their craft's nationality and registered keeper recorded by an authoritative organization. SSR can be applied for on line and is inexpensive.

<sup>6</sup> The European Commission and French Maritime Administration EQUASIS database provides this international type of transparency currently for commercial vessels.

## **6 International quality standards**

6.1 Member States and other authorities may wish to consider recommending the implementation of an appropriate quality standard which specifies the requirements for a security management system to ensure security in the supply chain.<sup>7</sup>

## **7 Assisting operators of non-SOLAS vessels to understand practices for interacting with ISPS Code-compliant vessels and port facilities**

7.1 Member States and other authorities may wish to assist the operators of non-SOLAS vessels to become aware of the security framework applying to ships and port facilities subject to SOLAS chapter XI-2 and the ISPS Code. Key aspects of this framework relevant to non-SOLAS vessels are:

- Awareness of security levels set by Contracting Governments;
- Requirements for interacting with ISPS-compliant vessels; and
- Requirements for interacting with ISPS-compliant port facilities.

7.2 Guidance on these three points is set out in paragraphs 3 and 4 of part 2.

## **8 ISPS Code as industry best practice for certain non-SOLAS vessels**

8.1 Member States and other authorities may wish to encourage operators of non-SOLAS vessels engaged on international voyages to adopt, where appropriate, the provisions of the ISPS Code as industry best practice.

---

<sup>7</sup> The ISO 28000 series of international standards is an example of such a quality standard.

## Appendix

### RISK ASSESSMENT AND MANAGEMENT TOOLS

#### 1 Introduction

1.1 The methodology presented herein includes five main phases:

- .1 **Threat assessment** – identifying the different threat scenarios and determining the likelihood of each occurring based on intent and capability.
- .2 **Impact assessment** – considering what the consequence of each threat scenario materializing would be and how much effect this would have.
- .3 **Vulnerability assessment** – determining what the key assets are and how they can be exploited, examining the mitigating controls in place and their effectiveness and considering residual weaknesses.
- .4 **Risk scoring** – making an assessment of the risk given all the factors noted in phases 1, 2 and 3.
- .5 **Risk management** – developing action plans, where appropriate, to address weaknesses and mitigate identified residual risks.

#### 2 Risk register and terminology

##### 2.1 The risk register

2.1.1 The risk register is a tool to document different scenarios and the associated findings on threat (likelihood based on intent and capability), impact, vulnerability and risk score. The format (at Table 1, below) is listed below along with accompanying explanations for each column. A step-by-step guide for completing the risk register follows the definition as well as details on the scoring mechanism.

**Table 1**

Reference number	Threat scenario	Lead organization	Support organizations	Threat (likelihood)	Impact	Vulnerability			Risk score
						Key assets	Mitigating controls	Vulnerability score	
1									
2									

Column 1: Reference number

- Each scenario should be listed with an assigned number so that it can be easily identified and its development tracked.

Column 2: Threat scenario

- This column is for the listing of the threat by name and a brief description of what it entails.

Column 3: Lead organization

- Each scenario needs to have a lead organization or coordinating body identified so that initial points of contact and responsibilities may be established.

Column 4: Support organizations

- List of those agents directly involved but not leading such as local police, fire departments, coast guards, etc.

Column 5: Threat (likelihood)

- This column gives the likelihood or probability of the situation coming to fruition if there were no security measures or mitigating controls in place to prevent them. It is scored on the basis of the intent and capability of those wishing to commit the act. Scoring for this element is explained later on in paragraph 3.4.

Column 6: Impact

- This column indicates the impact or consequence should the incident occur. Again scoring for this element is explained further in paragraph 4.

Column 7: Key assets

- This column contains a list of the most important resource key assets which could be affected by the scenario; this should include people, objects, physical infrastructure and equipment. By listing these assets a risk assessor is better able to consider what safeguards are in place and hence assess the vulnerability more accurately.

Column 8: Mitigating controls

- List and consider any mitigating controls (security measures) which are already in place to protect the key assets.

Column 9: Vulnerability score

- This is an assessment of the characteristics of a target or asset that can be exploited, balanced against mitigating controls (listed above). The scoring for this is also included later in paragraph 5.4 and considers what effect the mitigating controls have on the threat, the associated impact or both.

Column 10: Risk score

- All of the information gathered on threat, impact and vulnerability is used to score the risk. Groups or individuals should use the following formula to produce the score for each scenario:

$$\text{RISK} = \text{THREAT} \times \text{IMPACT} \times \text{VULNERABILITY}$$

### **3 Threat assessment**

#### **3.1 What to consider**

- Threat scenarios which could exist (or do exist);
- Who the lead and support organizations are for each scenario; and
- How to score accurately the threat and impact.

#### **3.2 Decide which threat scenarios apply**

3.2.1 The process should identify criminal acts which could take place.

3.2.2 The first task when completing a risk register is to consider and agree on which scenarios or events could apply.

3.2.3 It is useful to have a “brainstorming” session where subject matter experts consider:

- whether there are any additional scenarios, which should be listed; and
- any refinements needed to develop to the initial list.

3.2.4 It is useful when producing this list to consider potential perpetrators:

.1 Who are the groups and individuals who may act? For example:

- Terrorists
- Criminals
- Political groups
- Ideological groups
- Activists (e.g., animal rights/environmental)
- Disruptive passengers
- Employees
- Mentally unstable
- Those with inadequate documentation

.2 How do perpetrators operate?

.3 Some variables to consider in how they operate include:

- Reconnaissance, advanced planning; and
- Is there a precedent?

.4 What is their intent and their capability to act?

.4.1 Intent

- Definition: Motivation is what drives a perpetrator (e.g., financial gain, publicity, vengeance). Intent is who/what they want to harm to achieve their goal.

.4.2 Capability

Variables to consider include:

- numbers/organization
- status
- training
- funding
- weapons available
- track record
- support
- operational security

### **3.3 Decide lead and support organizations**

3.3.1 The lead organization(s) should either:

- .1 own the assets;
- .2 set the policy;
- .3 have legal responsibility for, or have the major role in, mitigating or responding to a particular threat; or
- .4 a combination of the above.

3.3.2 Distinctions should be made where appropriate between responsibilities for (i) preventive/protective security measures, (ii) contingency planning and reactive security measures to deal with and contain an incident, and (iii) implementation of the measures in (i) and (ii). There may be a different lead organization for each of these where responsibilities vary depending on type of threat, location and method.

3.3.3 Support organizations will be those which have a supporting role in mitigating the threat but don't meet the criteria above. The risk assessor may decide all stakeholders are support organizations in being vigilant, providing a deterring presence and sharing information with others.

- For some threats, identifying lead and support organizations is not a simple task. There may be differing views but it is important that consensus is reached, particularly as later on lead organizations will have a primary role in developing and delivering action plans, where these are necessary.

- There may, quite correctly, be more than one lead organization but if the group has listed several, it may be worth re-evaluating to check accuracy and minimize the potential for confusion and duplication.

### 3.4 Scoring the threat

- The score should reflect the likelihood of each of the threat scenarios in the register occurring if there were no security measures or mitigating controls in place to prevent them.

#### 3.4.1 Checklist

To accurately score the threat, assessors should:

- consider local and international intelligence/knowledge about similar events which have or could have occurred;
- discuss how likely it would be for each of the scenarios in the register to occur at the port if there were no security measures in place;
- read the definitions in Table 2 below and decide which score best applies. N.B. this is the score without any mitigating factors in place.

**Table 2 – Risk register – scoring definitions – threat**

Score	Likelihood	Criteria
4	PROBABLE	<ul style="list-style-type: none"> <li>✓ There have been previous reported incidents</li> <li>✓ There is intelligence to suggest that there are groups or individuals capable of causing undesired event</li> <li>✓ There is specific intelligence to suggest that the vessel or type of vessel is a target</li> </ul>
3	LIKELY	<ul style="list-style-type: none"> <li>✓ There have been previous reported incidents</li> <li>✓ There is intelligence to suggest that there are groups or individuals currently capable of causing undesired event</li> <li>✓ There is general intelligence to suggest that the vessel or type of vessel may be a likely target</li> </ul>
2	UNLIKELY	<ul style="list-style-type: none"> <li>✓ There is intelligence to suggest that there are groups or individuals capable of causing undesired event</li> <li>✓ There is nothing to suggest that the vessel or type of vessel is a target for the undesired event</li> </ul>
1	IMPROBABLE	<ul style="list-style-type: none"> <li>✓ There have been no previously reported incidents anywhere worldwide</li> <li>✓ There is no intelligence to suggest that there are groups or individuals capable of causing undesired event</li> </ul>

- The risk register is a template, rather than a straightjacket. Administrations are free to employ an alternative method of scoring if they find it produces a more logical and accurate assessment of the threats and risks.
- Remember to apply the agreed rules around confidentiality.

## 4 Impact assessment

### 4.1 Checklist

- List examples of the type and magnitude of impact that might be expected if the event happened; e.g., loss/damage to people, infrastructure, operations, finance or reputation;
- Assessors may wish to consider using or modifying the table at Table 3 below to record discussions. Note that the list of possible impacts highlighted below is not exhaustive.

**Table 3**

	<b>Loss of life</b>	<b>Personal injury</b>	<b>Loss/damage to vessel</b>	<b>Damage to vessel infrastructure</b>	<b>Loss of use of equipment</b>	<b>Disruption to services</b>	<b>Financial loss to vessel</b>	<b>Damage to reputation</b>	<b>Publicity to perpetrator</b>
<i>Improvised Explosive Device (IED)</i>									
<i>Sabotage</i>									
<i>Arson</i>									
<i>Unauthorized access</i>									
<i>Theft of vessels</i>									

4.2 This information should provide a robust basis for scoring. To score the impact accurately, groups or individuals should, in the same way as for threat:

- consider the impact should the event occur;
- consider the impact on the vessel (to safety, security, finance and reputation) of each of the risks occurring if there were there no security measures in place;
- consider how to record the scores allocated under each of the sub-headings. For simplicity an average may be taken in most cases. Where one score differs markedly from the other three it may be best to record it separately for future consideration rather than “losing” it in an average;
- read the definitions in Table 4 below and decide which one best applies (remember the score is without mitigating factors in place):

**Table 4 – Risk register – Scoring definitions – Impact**

<b>Score</b>	<b>Impact</b>	<b>Criteria</b>
4	SUBSTANTIAL	<ul style="list-style-type: none"> <li>✓ Potential for: multiple fatalities</li> <li>✓ Serious loss or damage to assets, infrastructure, vessel</li> <li>✓ Economic cost of more than (agreed figure)</li> <li>✓ Widespread coverage resulting in serious reputational damage</li> </ul>
3	SIGNIFICANT	<ul style="list-style-type: none"> <li>✓ Potential for: loss of life</li> <li>✓ Significant but repairable loss or damage to assets, infrastructure or craft</li> <li>✓ Economic cost of less than (agreed figure)</li> <li>✓ National adverse media coverage</li> </ul>
2	MODERATE	<ul style="list-style-type: none"> <li>✓ Potential for: major injuries</li> <li>✓ Short-term minor loss or damage</li> <li>✓ Economic cost of less than (agreed figure)</li> <li>✓ Major local reputational damage</li> </ul>
1	MINOR	<ul style="list-style-type: none"> <li>✓ Potential for: minor injuries</li> <li>✓ Minimal operational disruption</li> <li>✓ Economic cost of less than (agreed figure)</li> <li>✓ Minor reputational damage</li> </ul>

## **5 Vulnerability assessment**

The next step involves identifying the key assets or targets, their relevant characteristics and consideration of the controls in place to protect them and prevent criminal acts taking place. Assessors should first draw up a list of key assets that could be affected by a particular threat. This should include people (crew and passengers), objects and physical infrastructure.

### **5.1 Mitigating controls**

Identifying the current mitigating controls and assessing how effective they are is a vital but time consuming and intensive process. It may be useful to use the following processes:

### **5.2 Process mapping**

5.2.1 Drawing up process maps can be helpful in understanding complete processes, how each process works, who plays what role and what point, what the key points, strengths and weaknesses are and in identifying where and how aspects may be exploited.

5.2.2 The perceived benefits of process mapping are that it provides a genuinely holistic view of a process and is potentially a better way of:

- appreciating and accurately evaluating the various processes that take place;
- identifying synergies, duplication and gaps; and
- evaluating what action planning is required and how effective it is.

5.2.3 Rather than considering each threat separately, process mapping requires examination of the crime and security picture either:

- by article: vessel's stores; cargo; or
- by individual: crew or passengers.

5.2.4 Process mapping involves mapping the complete journey of a person or item and the evaluation and plotting of each potential threat, early warning indicator and mitigating measure in place. It should encompass all areas where and all times when the criminal act could be perpetrated.

### 5.3 Event cause analysis

5.3.1 This is a useful method to establish how a risk could materialize at the port and what areas of control need to work well.

5.3.2 Taking in turn the risks, the following five questions should be considered:

- What type of individuals or groups would want to carry out this event?
- Where is this event likely to take place? (Targeted at what?)
- How would it be carried out?
- What is going to deter or delay or detect or deal with them?
- What can go wrong? (e.g., poor communication).

5.3.3 Assessors may want to use the table in Table 5 below to note all this information down.

- This is a useful review tool to reconsider the effectiveness of control measures highlighted in the risk register and identify where there are weaknesses and gaps.

**Table 5**

<b>CONTROL MEASURES REVIEW</b> <b>Breach of Security</b>	<b>Possible Actions</b>
Security patrols Monitoring of security equipment Education and training of crew	Deterrence and Detection Pre-empt breach or Swift response Crew awareness
Inadequate resources Gaps in security coverage Insufficient training	Discuss issues with relevant personnel Consider redeployment of resources Organize crew training programme

5.3.4 Assessors may find it useful to complete Table 6, below, as they go through the Vulnerability stage.

- .1 What are the key targets – people, critical infrastructure, communications and control, and support services?

- .2 What are the systems designed to deter, detect, delay or deal with unlawful acts?
- .3 What are the weaknesses in these systems, including consideration of predictability and opportunity?

**Table 6**

Target	Strengths (i.e. systems in place to deter ...) <sup>*</sup>	Weaknesses <sup>**</sup>	Opportunities	Predictability	Target Vulnerability (High/Medium/Low)	What Stakeholders have a part to play in reducing the vulnerability of this target?	How?

**Key**

- Strengths = systems designed to deter, detect, or deal with unlawful acts;
- Weaknesses = includes things like limited intelligence to hand indicating the likelihood of attack and the desirability of the target for the perpetrator;
- Opportunities = opportunities for the perpetrator to exploit a loophole, conduct reconnaissance, etc.; and
- Predictability = the ways in which a target operates which make it predictable.

**\* Examples of systems designed to deter, detect or deal with unlawful acts**

- Company employee vetting system
- Port security vetting – pass system
- Criminal record checks
- Crew search and vehicle checks
- CCTV
- Restricted area, perimeter fencing and access control
- Control authority exercises
- Uniformed police presence
- Public awareness
- Cargo/catering/cleaning regimes
- Business continuity plans

\*\* **Examples of weaknesses**

- Accountability and funding
- Sheer volume of people and goods
- No searching (or regular searching)
- No search on exit as routine/norm
- Ability to respond to regulatory demands
- Exemptions in general (e.g., VIPs)
- Crew shortages
- Indifference
- Corruption
- Confusing legislation
- False documentation
- Poor surveillance

**Key issues to consider in vulnerability work**

- Need to consider high value assets
- Identify which stakeholders have a part to play in reducing the vulnerability of the target and how. This will assist in defining “who” should work together on what

**5.4 Vulnerability assessment and scoring**

5.4.1 Evaluation of targets’ characteristics on the one hand and the early warning indicators, embedded monitors and existing mitigating controls on the other should be translated into a vulnerability score. Table 7 below illustrates a possible scoring system to be used for assessing vulnerability:

**Table 7 – Access to sensitive area not inside boundary of RA**

4	No mitigating controls	No counter measures in place
3	Some mitigating controls	Some counter measures in place
2	Acceptable management of the risk	Measures in place sufficiently reasonable to manage the threat down to an acceptable level
1	Robust and effective counter measures	Full and complete counter measures in place

**6 Risk scoring**

**6.1 Risk score**

6.1.1 Finally, all of the information gathered on threat, impact and vulnerability should be used to identify and assess the residual risk. To score the risk accurately, groups or individuals should use the formula:

$$\text{RISK} = \text{THREAT} \times \text{IMPACT} \times \text{VULNERABILITY}$$

6.1.2 So, for example, using an initial threat score of 2, an impact score of 4 and, where there are no mitigating measures in place (a vulnerability score of 4) the residual risk score would be 32 (2 x 4 x 4 = 32). Where measures are adjudged to reduce the vulnerability to some extent,

but not to an acceptable level, the residual score would be 24. The threat and impact scores of 2 and 4 remain but the vulnerability score is now 3; hence  $2 \times 4 \times 3 = 24$ . And so on. There is a presumption that no threat scenario can be managed totally out of existence, i.e. you can never have a threat, impact or vulnerability score of 0.

6.1.3 It should be noted that scenarios with differing individual threat, impact and vulnerability scores can have the same overall risk score. For instance a particular scenario may have a threat score of 2 an impact score of 2 and a vulnerability score of 2 whereas another scenario may have a threat score of 1, an impact score of 4 and a vulnerability score of 4. Both scenarios produce a risk score of 16 despite having differing individual values of threat, impact and vulnerability.

6.1.4 Risk can then be ranked into three broad categories: high, medium and low:

- HIGH - A residual risk score of 27 or more.
- MEDIUM - A residual risk score of between 8 and 24.
- LOW - A residual risk score of 6 or less.

## 7 Risk management

7.1 The risk management phase considers how best to address the weaknesses identified during the vulnerability and risk scoring stages and how to mitigate the risk effectively and practically on a sustainable long-term basis.

7.2 This can be achieved by all stakeholders working together to agree joint tactical action plans. The checklist below gives some pointers on how to work through the process:

### 7.3 Drawing up action plans

- Consider the overall risk profile from the risk register:
  - High = Unacceptable Risk – seek alternative and/or additional control measures,
  - Medium = Manageable risk – requires management/monitoring,
  - Low = Tolerable risk – no further control measures needed.
- Reconsider the Control Measures Review table. The “concerns” and “do nexts” should assist in drawing up action plans.
- Agree the priorities for action. These should be the “high” risks in the first instance.
- Identify what actions can and need to be taken to bring the risk down to a “medium”: manageable risk and from there to a “low”: tolerable risk.
- Agree who will be the lead agency in implementing changes.
- Consider the resource implications.
- Document recommendations.
- Document actions taken and link these back to the threats in the risk register:
  - Timetable for action
  - Review of actions
- Agreed actions should be recorded and progress monitored. Such records are also evidence of decisions taken.
- Assessors may need to develop further systems for sharing information and intelligence.
- Look for opportunities to share resources and assist others.

7.4 Actions will probably fall into the following categories:

- Actions that may be implemented by the group;
- Tactical or operational issues; and
- National, policy or strategic issues.

## **8 Re-evaluation**

8.1 Risk assessments should be reviewed as conditions change, or on a regular schedule (e.g., annually).

## **Part 2: Information for use by owners, operators and users (operators) of non-SOLAS vessels and related facilities**

### **1 Risk assessment**

1.1 The implementation of security measures for non-SOLAS vessel operations should be informed by a risk assessment. Such a risk assessment<sup>8</sup> may be conducted by Member States or other authorities or by the vessel owners, operators and users.

1.2 A tool to assist with undertaking risk assessments is attached as the Appendix to annex 1.

### **2 Maintaining security awareness and reporting suspicious activity**

2.1 Operators of non-SOLAS vessels may wish to provide all personnel with information on how to reach appropriate officials and authorities in the event of security problems or if suspicious activity is observed.<sup>9</sup> This information should include contact information for the officials responsible for emergency response, the national response centre(s) (if appropriate) and any authorities that may need to be notified.

2.2 Operators of non-SOLAS vessels and relevant organizations may wish to engage with Member States and other authorities in developing security initiatives with respect to education, information sharing, coordination, and outreach programmes. Such engagement could be considered toward establishing programmes to improve vessel operators' security awareness and to promoting links with Administration maritime security services.

2.3 Entities responsible for establishing and maintaining security awareness and culture should be mindful of the need for the proper balance between the needs of security and the requirement to maintain the safe and working efficiency of vessels. Vessel operators should take into account the Human Element and the rights and welfare of seafarers and maritime workers, including the relevant provisions of the ISPS Code, when implementing these Guidelines.

### **3 Awareness of basic security requirements of SOLAS chapter XI-2 and the ISPS Code**

3.1 The ISPS Code defines three Security Levels:

- Security Level 1: Normal
- Security Level 2: Heightened
- Security Level 3: Exceptional

---

<sup>8</sup> Examples of guidance and tools for undertaking a risk assessment of vessels may be found in:

- ILO/IMO Code of Practice on Security in Ports.
- MSC.1/Circ.1193: Guidance on voluntary self-assessment by Administrations and for ship security.
- American Bureau of Shipping: Ship Security Plan Review Checklist.
- United States Coast Guard Navigation and Vessel Inspection Circular 10-02: Security Guidelines for Vessels.
- Norwegian Shipowners' Association: Guideline for performing Ship Security Assessment.

<sup>9</sup> Examples of suspicious activity can be found at paragraph 7.2.4 of this annex.

3.2 At Security Level 1, vessels and port facilities are required to have basic security measures in place. Security Level 2 represents a heightened level of threat, and vessels and port facilities are required to increase their levels of protective security. Security Level 3 represents an imminent and specific threat, and vessels and port facilities will be required to increase security provision still further and respond to instructions from relevant control authorities.

3.3 Part of the IMO requirement is that all ISPS-compliant port facilities and ships create and maintain a Port Facility Security Plan (PFSP) or a Ship Security Plan (SSP). Security measures and standards should be developed on the basis of security assessments.

#### **4 Awareness of basic requirements for interacting with ISPS-compliant ships and port facilities**

##### **4.1 Interacting with ISPS-compliant ships**

4.1.1 Operators of non-SOLAS vessels should be aware of the requirements of SOLAS chapter XI-2 and the ISPS Code, which apply to all ships engaged on international voyages of 500 gross tonnage and above or those which carry more than 12 passengers, for interacting with ISPS-compliant ships. Non-SOLAS vessels may be required to complete a “Declaration of Security” (DoS) when interfacing with an ISPS-compliant ship. The purpose of the DoS is to ensure that agreement is reached on the respective security measures each will undertake under such circumstances.

4.1.2 When there is a requirement for non-SOLAS vessels to enter into a DoS, the operator of the non-SOLAS vessel may expect the following procedures to be applied:

- the ISPS-compliant ship should contact the non-SOLAS vessel well in advance of the non-SOLAS vessel’s interaction with the ISPS-compliant ship, giving the master of the non-SOLAS vessel reasonable time to prepare for those security measures that might be required;
- the Ship Security Officer for the ISPS-compliant ship should detail the security measures which the non-SOLAS vessel is being asked to comply with;
- the agreed details of security measures to be implemented should be inserted into a DoS using the appropriate form;
- the DoS should be completed and signed by both parties.

4.1.3 It is important that all operators of non-SOLAS vessels are aware of the need to stay a reasonable distance from ISPS-compliant ships when using shared waterways. The appropriate distance will vary due to navigational safety considerations. Non-SOLAS vessels should take care not to undertake any manoeuvres close to the vessel which may give the crew of the ISPS-compliant ship cause for concern. Non-SOLAS vessels are encouraged to clearly indicate their intentions to the crew of the ISPS-compliant ship by radiotelephone or other means.

##### **4.2 Interacting with ISPS-compliant port facilities**

4.2.1 Operators of non-SOLAS vessels should be made aware of the requirements for interacting with ISPS-compliant port facilities. Non-SOLAS vessels may be required to complete a DoS when arriving at an ISPS-compliant port facility. The purpose of the DoS is to ensure that agreement is reached on the respective security measures each will undertake under such circumstances.

4.2.2 When there is a requirement for non-SOLAS vessels to enter into a DoS, the Port Facility Security Officer of the regulated facility should follow the procedures below:

- the ISPS-compliant port facility should contact the non-SOLAS vessel well in advance of the non-SOLAS vessel's interaction with the ISPS-compliant port facility, giving the master of the non-SOLAS vessel reasonable time to prepare for those security measures that might be required;
- the Port Facility Security Officer for the ISPS-compliant port facility should detail the security measures which the non-SOLAS vessel is being asked to comply with;
- the agreed details of security measures to be implemented should be inserted into a DoS using the appropriate form; and
- the DoS should be completed and signed by both parties.

## **5 Training and personnel practices**

5.1 Operators of non-SOLAS vessels may wish to develop security policies and procedures, taking into consideration security assessments, to ensure that all personnel (including passengers where appropriate) are familiar with basic security measures applicable to the vessel.

5.2 Basic security familiarization training is recommended for crew members enabling them to have the capability to respond to security threats. In higher-risk environments, this training should also have the purpose of testing and assessing competence and knowledge for effective implementation of the recommendatory security measures contained in these Guidelines. Crew members operating in higher-risk environments could receive additional security familiarization training to enable them to better respond to specific security threats.

5.3 Operator proficiency training for pleasure craft owners and operators could encompass security awareness familiarization.

5.4 Hiring practices, such as reference checking, which might include background checks, can help a company identify potential security threats from employees. Seafarers and other workers should be allowed to appeal adverse employment determinations that are based upon disputed background information. There should also be adequate protections for workers' rights to privacy.

## **6 Security measures**

### **6.1 Mitigating the risk of theft, piracy and armed robbery against non-SOLAS vessels<sup>10</sup>**

6.1.1 Operators of non-SOLAS vessels should consider the risk to the vessel of theft, piracy and armed robbery and mitigate the risk by implementing appropriate security measures. The following are examples of good practice which may be implemented to reduce the likelihood of theft, piracy and armed robbery against non-SOLAS vessels:

---

<sup>10</sup> Operators may wish to apply the guidance given in MSC/Circ.622/Rev.[2] on Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships, and MSC/Circ.623/Rev.[4] on Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships.

i) **Be vigilant**

Early detection of a possible attack is the most effective deterrent. The majority of attacks will be deterred if the robbers/hijackers are aware that they have been observed. Advance warning of a possible attack will give the opportunity to sound alarms, alert coastal authorities, undertake evasive manoeuvring where possible, secure access points to the vessel and where appropriate and possible prepare defences such as water hoses. Pirates and armed robbers are usually well organized and equipped with weapons. Crew should not display aggressive responses, once an attempted boarding or attack is underway and, in particular, once the attackers have boarded the vessel, as this could significantly increase the risk to the vessel and those on board.

ii) **Maintain a 24-hour visual and security watch**

Security watch includes short range radar surveillance of the waters around the vessel. The use of a small marine radar, fitted in such a way to ensure complete coverage of the stern, un-obscured by the radar shadow of the vessel itself, should be considered. Keep a special look-out for small boats and fishing boats that attackers often use because they are difficult to observe on radar. In piracy “hotspots”, discourage passengers and crew from trading with locals using small craft which may approach the vessel.

iii) **Strengthen night watches**

Strengthen night watches especially around the rear of the vessel and anchor chains/mooring ropes and particularly between the hours of 0100 and 0600 when most attacks occur. Continuous patrols linked by “walkie-talkie” to the bridge should be established, especially in high risk ports of transit areas. A drill should be established for regular two-way communication between the watch and the bridge. If possible, an additional officer should assist the normal bridge watch keepers at night, in order to provide a dedicated radar and visual watch for small craft that might attempt to manoeuvre alongside, and allow the watch keepers to concentrate on normal navigational duties. Night patrols of the vessel should be staggered to avoid forming patterns which an adversary could observe.

iv) **Seal off means of access to the vessel**

Fit hawse pipe plates, lock doors and secure hatches, etc. While taking due account of the need for escape in the event of fire or other emergency, so far as possible all means of access to the accommodation should be sealed off and portholes and doors of crew members’ quarters should be secured at all times. Where applicable blocking access between the aft deck and the crew members’ quarters is particularly important.

v) **Establish radio contact**

Establish radio contact and agree on emergency signals specifically for attacks with crew, shore authorities, etc.

vi) **Provide adequate lighting**

Deck and over-side lights, particularly at the bow and stern, should be provided to illuminate the deck and the waters beyond and to dazzle potential boarders. Searchlights should be available on the bridge wings, and torches should be carried by the security patrols to identify suspicious craft. Such additional lighting should not however be so bright as to obscure navigation lights or interfere with the safe navigation of other vessels.

vii) **Evasive manoeuvring**

Provided that navigational safety allows, Masters may consider “riding off” attacking vessels by heavy wheel movements as they approach or by attempting to out run the attackers vessel. The effect of evasive manoeuvring may deter would-be attackers and make it difficult for them to attach poles or grappling devices.

viii) **Water hoses and other equipment**

A vessel’s rear deck is vulnerable to attempted boarding by robbers/hijackers and as an option can be sprayed with water to deter an attempted boarding. The use of water hoses to deter boarding of robbers/hijackers should only be considered if the Master is convinced he can use them to advantage, and without risk of provoking reprisals from the attackers. Consider fitting or equipping the vessel with passive security/detection equipment, e.g., Perimeter Intruder Detection Systems, CCTV, Night Vision equipment. Where possible, such equipment should be linked to an alarm system.

ix) **Reduce opportunities for theft**

Remove all portable equipment from the deck, so far as is possible stow containers containing valuables door-to-door and in tiers, and seal off access to accommodations.

x) **Establish a secure area(s)**

If large numbers of armed robbers/hijackers succeed in boarding the vessel, it may be necessary for crewmembers and passengers to retreat to a secure area(s). Depending upon the construction of the accommodations and the extent to which areas can be effectively sealed off, such a secure area should be identified in advance. Provision should be made, however, for escape during a fire or other emergency.

## **6.2 Preventing unauthorized access to the vessel**

6.2.1 Guidance on preventing unauthorized access to each of the four non-SOLAS vessel categories is set out in the Appendices.

### 6.3 Conducting a search of a vessel

6.3.1 The following are examples of good practice which should be implemented to assist crew undertaking patrolling duties when operating in a higher-risk environment:

- **Define the search area** – crew members should be fully briefed and aware of what is required and have clearly defined start and finish points.
- **Plans** – laminated plans of search areas should be produced in advance, highlighting the key features of the areas to be searched (such as storage bins and emergency exits).
- **Thoroughness** – thorough searches help detect concealed items and attention should be paid to vulnerable areas. Crew should not rely solely on visual checks, but should take note of unusual sounds, smells, etc.
- **Use of seals** – un-lockable equipment boxes such as lifejacket boxes can be fitted with tamper evident seals eliminating the need to search inside unless the seal is no longer intact.
- **Pre-planned action** – crew members should be fully briefed on their expected actions in the event a search identifies a security concern.

### 6.4 Verifying identity of persons on board a vessel

6.4.1 The following are examples of good practice which could be implemented to verify the identity of persons on board a vessel when operating in a higher-risk environment:

- All visitors (other than passengers) should report to the Master of the vessel, or other responsible person, to notify them of their arrival and departure. All visitors should have a form of identity, for example an ID card, passport or some other form of identification bearing the individual's photograph.
- Passengers must present a valid ticket before boarding (except where tickets are bought on board the vessel) and where applicable have a form of identity such as an ID card, passport or some other form of identification bearing the individual's photograph. For chartered vessels where no tickets are required, the chartering party should give some thought as to how they will control access. This could be achieved through the provision of paper authorization such as an invitation to be shown or for names on a list to be checked off on presentation of identification.

## 7 Planning for security events

### 7.1 Responding to bomb threats or discovery of suspicious items

7.1.1 Bomb threats are usually anonymous and communicated by telephone. While bomb threats are usually hoaxes intended to cause a nuisance, they must be taken seriously as a small number have been genuine and have preceded a terrorist or criminal act. It is recommended that advice is sought from local authorities on how to handle any genuine bomb threats that may be received.

7.1.2 Plans and procedures should be in place for dealing with health and safety alerts both on a vessel and at piers. These plans may be adapted to cover security alerts. Responsible individuals should consider various possible scenarios and appropriate responses. Scenarios could include:

- i) Suspect packages found on board a vessel or at a pier;
- ii) Individuals behaving suspiciously either on a vessel or at a pier;

- iii) Security alert at another pier or on another vessel requiring suspension of operations; and
- iv) A direct attack against a vessel or pier by unknown persons which could include ramming or the successful explosion of an Improvised Explosive Device.

7.1.3 Responsible individuals should similarly consider how to isolate a suspect package if found without removing or touching it and how to evacuate the vessel and piers quickly and safely. Planning should include being aware of who to contact, such as the police, emergency services, or other operators and how to document the incident.

7.1.4 Any Guidelines relating to management of bomb threats should include contact details for police or other public authorities responsible for immediate actions in the event of bomb threats.

## **7.2 Maintaining a means for reporting security concerns**

7.2.1 Operators of non-SOLAS vessels should provide all personnel with contact information for authorities responsible for emergency response, the national response centre(s) (if appropriate) and any other authorities that may need to be notified.

7.2.2 Operators of non-SOLAS vessels should consider and identify the actions that crew members should take in the event of a security incident. Such actions might include:

- what the crew should do when a vessel is moored or underway;
- how to notify authorities that a security incident is taking place (e.g., making radio calls, sounding alarms, etc.); and
- how crew members should protect themselves, their vessel and the public.

7.2.3 Reports of security incidents on board a vessel should be reported to the Master or Vessel Security Officer as appropriate.

7.2.4 All personnel should report suspicious activities to appropriate authorities. The report should include details of the activity and its location. The list below gives examples of activities which may by themselves constitute suspicious behaviour, any one of which may be considered suspicious by itself. However, those suspicions may warrant particular attention when one or more behaviour or a pattern of behaviour is observed or detected. The list is not exhaustive.

- i) Information gathering activities:
  - Unknown persons photographing vessels or facilities.
  - Unknown persons contacting, by any media, a ship or facility for the purpose of ascertaining security, personnel or standard operating procedures.
  - Unknown persons attempting to gain information about vessels or facilities by walking up to ship or facility personnel or associated individuals, or their families, and engaging them in conversation.
  - Theft or the unexplained absence of standard operating procedures documents.

- ii) Attempted inappropriate access:
  - Inappropriate or unauthorized persons attempting to gain access to vessels or facilities.
  - Unknown or unauthorized workmen trying to gain access to facilities to repair, replace, service, install or remove equipment.
  
- iii) Activities in a port and its environs:
  - Theft of facility vehicles, vehicle passes, personnel identification or personnel uniforms.
  - Inappropriate use of Global Maritime Distress Safety and Security procedures.
  - Suspicious individuals establishing *ad hoc* businesses or roadside stands either adjacent to or in proximity of port facilities.
  - Repeated or suspicious out of ordinary attempts at communication by voice media with duty personnel.
  - Vehicles or small vessels loitering in the vicinity of a facility without due cause for extended periods of time.
  - Unknown persons loitering in the vicinity of a facility without due cause for extended periods of time.<sup>11</sup>

### **7.3 Prevention of trafficking in drugs and transportation of illicit cargoes**

7.3.1 The following are general Guidelines for precautionary measures which may be taken to safeguard a non-SOLAS vessel while in port, irrespective of whether at anchor or alongside a berth, to protect the vessel against trafficking in drugs and the transportation of illicit cargoes:

- The crew should be warned about the risks of knowingly transporting illicit cargoes and trafficking in drugs.
- Crew going ashore should be advised that they should take care to ensure that persons they are meeting with are not connected with illegal activities.
- The vessel might maintain a security log book at the point of entry/exit to the vessel, recording the identity of all persons boarding or disembarking. No unauthorized persons should be allowed to board.
- A permanent watch may be advisable in working areas. If appropriate, areas such as the forecabin, poop deck, main decks, etc., must be well lit during the hours of darkness.
- The vessel should maintain a good lookout for approaching small boats, or the presence of unauthorized divers, or other attempts by unauthorized persons to board the vessel.
- In the event of drugs or illicit cargoes are found on board, the crew should cooperate fully with the local authorities for the duration of the investigation.

---

<sup>11</sup> Lawful gatherings and assemblies should not be misconstrued as being suspicious.

## 7.4 Prevention of stowaways

7.4.1 For the purposes of the Guidelines a stowaway is defined as a person who is secreted on a vessel, or in cargo which is subsequently loaded onto a vessel, without the consent of the vessel owner or the master or other responsible person, and who is detected on board after the vessel has departed from a port and is reported as a stowaway by the master to the appropriate authorities.

7.4.2 The visible actions of the crew in implementing security measures will act as a deterrent to potential stowaways. Examples of general precautionary measures for the prevention of stowaways are set out below:

- Prior to entering port, doors and hatchways should be securely fastened and locked with due regard to the need to facilitate escape in the event of an emergency.
- Fitting plates over anchor hawse pipes can prevent stowaways from boarding at anchorage or before a vessel is berthed.
- Accommodation doors could also be secured and locked, leaving only one open entrance. In the interests of safety, keys to the locked doors should be placed in convenient positions so that doors can be opened in the event of emergency.
- Store rooms, equipment lockers on deck, the engine room and the accommodations should remain locked throughout a port call, only being opened for access and re-secured immediately thereafter.
- Once alongside, a gangway watch is the first line of defence against stowaways, smugglers and theft. For this reason, it is important to ensure that an effective gangway watch is maintained at all times.
- At the commencement of loading only the hold access doors of the compartments that are going to be used for the immediate loading of cargo should be opened. As soon as cargo operations cease, the compartment should be secured.
- The vessel's storerooms should also be kept locked at all times, only being opened when access is required.
- There may be some areas of the vessel that cannot be locked, for instance the funnel top. Any unlocked areas that can be accessed should be inspected on a regular basis.
- On completion of cargo loading operations and the disembarkation of all shore-based personnel, accessible areas of the vessel should be searched again.
- In high-risk ports consideration should be given to anchoring in some convenient position outside the port and making a final stowaway search after tugs and pilots depart.

7.4.3 A detected stowaway should be reported to the appropriate authorities. Any stowaways detected should be treated in accordance with humanitarian principles. However, some stowaways may be violent, and the safety and security of the vessel and its crew should not be compromised.

## **Appendix A**

### **GUIDELINES FOR COMMERCIAL NON-PASSENGER VESSELS**

#### **Introduction**

These Guidelines apply to all commercial non-passenger vessels and special purpose vessels that fall outside the requirements of the International Ship and Port Facility Security (ISPS) Code.

The Guidelines are intended to provide information and best practice guidance to operators of non-SOLAS vessels. They are not mandatory and are not intended to form the basis for a mandatory instrument.

#### **Vessel security**

##### **1 Searching**

The vessel should be searched to ensure that nothing illegal or harmful has been placed on board. The vessel should be searched at the end of an outward trip before starting the return voyage to ensure that nothing has been concealed or left behind. To the extent possible, checks should include any crew areas, stores, holds, underwater hull if concern prevails and areas that could conceal persons or articles that may be used for illegal purposes.

There should be agreed procedures on how to isolate a suspect package if found and how to evacuate the vessel quickly and safely.

##### **2 Securing**

With due regard to the need to facilitate escape in the event of an emergency, external doors and storage areas should be locked and portholes secured. If the vessel is to be left unattended for a lengthy period of time such as overnight, it is recommended that the engine is disabled to prevent theft/unauthorized use and that it is moored securely in compliance with local port by-laws. Masters should ensure that the gangway is raised when the vessel is left unattended.

##### **3 Preventing unauthorized access to vessels**

Members of the public should not be able to gain access to operational areas of the vessel, or maintenance/storage facility such as crew rest rooms, store rooms, cleaning cupboards, hatches and lockers. All doors leading into operational areas should be kept locked or controlled to prevent unauthorized access. The only exception to this should be where access is required to reach safety equipment or to use emergency escapes. Keys for doors should be kept in a secure location and controlled by a responsible person. If access is controlled by keypad, the code should only be given to people with a legitimate need to know. It is also recommended that codes are changed periodically. Where such access controls are in place, crew should be reminded of the importance of ensuring that nobody following can bypass the access controls.

The following are suggested measures to deter unauthorized access to the vessel:

- over-the-side lighting which gives an even distribution of light on the whole hull and waterline

- keeping a good watch from the deck
- challenging all approaching boats. If unidentified, they should, where possible, be prevented from coming alongside.

#### **4 Controlling access**

All visitors should report to the Master of the vessel, or other responsible person to notify them of their arrival. It is recommended that they be advised on security procedures, such as the following:

- The need to be escorted at all times;
- The need to wear a permit, if issued, at all times;
- The need for vigilance at all times when on the vessel. Should they find a suspicious item, they should not touch it but should contact a member of crew as soon as possible. Similarly, they should contact a member of crew if they see a person acting suspiciously; and
- The need to secure all doors behind them when leaving, particularly those doors which lead to operational areas of the vessel. If they are leaving a work site, they must ensure that it is locked and that all equipment has been securely stored.

The vessel might maintain a security log book at the point of entry/exit to the vessel, recording the identity of all persons boarding or disembarking.

#### **5 Contingency measures for security alerts**

Contingency measures should be in place for dealing with emergency navigational and health and safety alerts on board vessels. These plans may be adapted to include procedures for security alerts and incidents.

If a suspicious device or package is found while a vessel is at sea, the master should take into account:

- the size and location of the device;
- the credibility of the threat;
- the vessel's location and the time it will take for security services and other assistance to arrive;
- the need to keep everyone well clear of the suspect device; and
- the need for all on board to keep clear of all doors, trunks and hatches leading from the space containing the device to avoid possible blast injuries.

#### **6 Reporting security incidents**

Vessel operators should implement procedures and processes for reporting and recording security incidents.

In the event of a security incident occurring while the vessel is at sea the master, in addition to activating an appropriate response, should alert the nearest coastal State or authorities and/or vessels in vicinity and provide details of the incident.

## **Appendix B**

### **GUIDELINES FOR NON-SOLAS PASSENGER VESSELS**

#### **Introduction**

These Guidelines apply to all passenger vessels that fall outside the requirements of the International Ship and Port Facility Security (ISPS) Code.

The Guidelines are intended to provide information and best practice guidance to operators of non-SOLAS passenger vessels. They are not mandatory and are not intended to form the basis for a mandatory instrument.

Terrorists perceive passenger vessels and ferries as attractive targets because they carry large numbers of people, are high profile and economically important.

Given that information on schedules, routes and vessel schematics are all readily available, these vessels may be more vulnerable to attack.

#### **Vessel security**

##### **1 Searching**

The vessel should be searched to ensure that nothing illegal or harmful has been placed on board. The vessel should be searched at the end of an outward trip before starting the return voyage to ensure that nothing has been concealed or left behind. It is recommended that passengers are not permitted to board until the security check of the vessel has been completed. To the extent possible, checks should include all public areas with special attention paid to underneath seating, toilets, and any storage areas, e.g., for luggage, on the vessel. To the extent possible, checks should include any crew areas, stores, holds, under-water hull if concern prevails and areas that could conceal persons or articles that may be used for illegal purposes.

There should be agreed procedures on how to isolate a suspect package if found and how to evacuate the vessel quickly and safely.

##### **2 Securing**

With due regard to the need to facilitate escape in the event of an emergency, external doors and storage areas should be locked and portholes secured. If the vessel is to be left unattended for a lengthy period of time such as overnight, it is recommended that the engine is disabled to prevent theft/unauthorized use and that it is moored securely in compliance with local port by-laws. Masters should ensure that the gangway is raised when the vessel is left unattended.

##### **3 Control of passengers boarding and disembarking**

Passengers must only be allowed to embark and disembark if crew or shore staff are present. Where ticket facilities exist for scheduled services, crew or shore staff should ensure that passengers present valid tickets before boarding. For chartered vessels where no tickets are

required, the chartering party should seek to control access on to the boat, for example through the provision of an authorization card. If the vessel carries vehicles special additional measures, including spot checks, may be required.

#### **4 Passenger security awareness**

Passengers should be reminded not to leave bags unattended and to report any unattended or suspect packages. Security messages should be displayed on posters and information screens and should be frequently delivered over public address systems either as separate announcements or as part of the pre-sailing safety announcement.

#### **5 Preventing unauthorized access to vessels**

Passengers should not be able to gain access to operational areas of the vessel, or maintenance/storage facility such as crew rest rooms, store rooms, cleaning cupboards, hatches and lockers. All doors leading into operational areas should be kept locked or controlled to prevent unauthorized access. The only exception to this should be where access is required to reach safety equipment or to use emergency escapes. Keys for doors should be kept in a secure location and controlled by a responsible person. If access is controlled by keypad, the code should only be given to people with a legitimate need to know. It is also recommended that codes are changed periodically. Where such access controls are in place, crew should be reminded of the importance of ensuring that nobody following can bypass the access controls.

The following are suggested measures to deter unauthorized access to the vessel:

- over-the-side lighting which gives an even distribution of light on the whole hull and waterline;
- keeping a good watch from the deck; and
- challenging all approaching boats. If unidentified, they should, where possible, be prevented from coming alongside.

#### **6 Controlling access**

All visitors (other than passengers) should report to the master of the vessel, or other responsible person to notify them of their arrival. It is recommended that they should be advised on security procedures, such as the following:

- The need to be escorted at all times;
- The need to wear a permit, if issued, at all times;
- The need for vigilance at all times when on the vessel. Should they find a suspicious item, they should not touch it but should contact a member of crew as soon as possible. Similarly, they should contact a member of crew if they see a person acting suspiciously; and
- The need to secure all doors behind them when leaving, particularly those doors which lead to operational areas of the vessel. If they are leaving a work site, they must ensure that it is locked and that all equipment has been securely stored.

## **7 Contingency measures for security alerts**

Contingency measures should be in place for dealing with emergency navigational and health and safety alerts on board vessels. These plans may be adapted to include procedures for security alerts and incidents.

If a suspicious device or package is found while a vessel is at sea, the master should take into account:

- the size and location of the device;
- the credibility of the threat;
- the vessel's location and the time it will take for security services and other assistance to arrive;
- the need to keep everyone well clear of the suspect device; and
- the need for all on board to keep clear of all doors, trunks and hatches leading from the space containing the device to avoid possible blast injuries.

## **8 Reporting security incidents**

Vessel operators should implement procedures and processes for reporting and recording security incidents.

In the event of a security incident occurring while the vessel is at sea the master, in addition to activating an appropriate response, should alert the nearest coastal State or authorities and/or vessels in vicinity and provide details of the incident.

## **Appendix C**

### **GUIDELINES FOR FISHING VESSELS**

#### **Introduction**

These Guidelines apply to fishing vessels.

The Guidelines are intended to provide information and best practice guidance to operators of fishing vessels. They are not mandatory and are not intended to form the basis for a mandatory instrument.

The operator, as well as the master of a fishing vessel should evaluate and enforce appropriate measures as provided for in this annex, taking into consideration the security environment and the risk areas related to the operating area and the security risk that may be encountered during the intended voyage.

#### **Vessel security**

##### **1 Searching**

Vessels should be searched after having been left unattended to ensure that nothing has been placed aboard while the vessel was unattended and for the purpose of concealing trespassing persons and articles placed on board for illegal purposes. To the extent possible, checks should include all spaces accessible to non-authorized persons while the vessel was unattended, e.g., any crew areas stores, holds, under-water hull, if concern prevails and areas that could conceal persons or articles that may be used for illegal purposes.

##### **2 Securing**

With due regard to the need to facilitate escape in the event of an emergency, where possible external doors, hatches and storage areas should be kept locked and windows secured while the ship is left unattended. If the vessel is left unattended for a lengthy period of time such as overnight, it is recommended that the engine is disabled to prevent theft/unauthorized use.

##### **3 Preventing unauthorized access to vessels**

Measures preventing unauthorized access to vessels should be implemented and maintained. Such measures could be:

- over-the-side lighting which gives an even distribution of light on the whole hull and waterline;
- keeping a good watch from the deck;
- challenging all approaching boats. If unidentified, they should, where possible, be prevented from coming alongside; and
- all visitors and contractors should report to the master of the vessel, or other responsible person to notify them of their arrival.

#### **4 Contingency measures for security alerts**

Contingency measures should be in place for dealing with emergency navigational and health and safety alerts on board vessels. These plans may be adapted to include procedures for security alerts and incidents.

If a suspicious device or package is found while a vessel is at sea, the master should take into account:

- the size and location of the device;
- the credibility of the threat;
- the vessel's location and the time it will take for security services and other assistance to arrive;
- the need to keep everyone well clear of the suspect device; and
- the need for all on board to keep clear of all doors, trunks and hatches leading from the space containing the device to avoid possible blast injuries.

#### **5 Reporting security incidents**

Vessel operators should implement procedures and processes for reporting and recording security incidents.

In the event of a security incident occurring while the vessel is at sea the master, in addition to activating an appropriate response, should alert the nearest coastal State or authorities and/or vessels in vicinity and provide details of the incident.

## **Appendix D**

### **GUIDELINES FOR PLEASURE CRAFT**

#### **1 Introduction**

These Guidelines apply to pleasure craft. Pleasure craft, recreational vessels, and leisure craft (hereinafter referred to as pleasure craft) are vessels which are not subject to the International Convention for the Safety of Life at Sea (SOLAS) and do not routinely engage in commercial activities such as carrying cargo or passengers for hire. This class of vessels might also encompass vessels being used as residences provided the vessel maintains a means of propulsion.

The International Maritime Organization does not define the term pleasure craft in the Convention on the International Regulations for Preventing Collisions at Sea, 1972 (COLREGs). Each Member State will have its own definition and may apply these Guidelines as appropriate.

The pleasure craft sector is generally less regulated than SOLAS Convention and ISPS-regulated vessels, and where regulations do exist they are mainly focused on safety. However, pleasure craft frequently use the same waters as other vessels and while the vast majority of pleasure craft are operated by legitimate, law-abiding owners and operators, they may be used for criminal objectives and terrorism.

The Guidelines are intended to provide information and best practice guidance to operators of pleasure craft. However, pleasure craft owners and operators should remember that the overall safety and security of the vessel, crew, and passengers is their responsibility. Prudent mariners are proactive in preventing incidents, planning in advance how best to respond to an incident, and ensuring that all passengers and crew members know their roles.

The Guidelines are not mandatory and are not intended to form the basis for a mandatory instrument.

#### **2 Applicability**

The primary focuses of this appendix are pleasure craft operating in waters where they might interact with or operate in close proximity to vessels or facilities subject to SOLAS chapter XI-2 and the ISPS Code; and also those pleasure craft engaged in international voyages. However, where appropriate, Member States, based on their assessed levels of threat and risk, may consider broader implementation as many pleasure craft are highly mobile, both via land and connecting waterways.

#### **General security guidelines**

3 The best security is preventative security. Pleasure craft owners and operators are encouraged to consider their security relevant to their intended area of operations and when passage planning to ensure that all onboard are aware of their roles and responsibilities. Pleasure craft owners and operators should be familiar with any particular directions that exist for an intended port or destination. This information is available in nautical almanacs, notices to mariners and from harbour authority and administration websites.

4 Pleasure craft should be checked by their owners or operators at regular intervals, to ensure that nothing has been placed aboard or removed while the vessel has been unattended. In the event that something suspicious is found, the appropriate local authorities should be notified promptly. Pleasure craft operators should not, under any circumstances, directly handle suspicious packages or objects but should follow any instructions from notified authorities with respect to evacuation of the vessel and the area around it.

5 Where possible, external doors, hatches and storage areas should be locked and windows secured when a pleasure craft will be left unattended. If a vessel is to be left unattended for some time, it is recommended that steps be taken to prevent theft or unauthorized use, and that the vessel is moored securely in compliance with local rules or regulations. Such security steps could include:

- Ignition switches should be locked.
- Consider fitting a small craft alarm system, possibly with an autodial facility to alert an operator to any unauthorized movement, or the activation of a variety of on board security sensors, via Cell Phone or e-mail. The alarm system could also be integrated with smoke and fire sensors for a complete vessel protection system.
- Consider securing high value items such as televisions, DVDs, etc., so that they are out of sight and in lockable compartments.
- Never leave anything valuable on display. Valuables that can be removed should be taken home not put in cupboards.
- Consider using steering locks if practical.
- Mark all your equipment where possible with your details using approved property marking equipment.
- Consider etching the hull identification number onto windows and hatches.
- When you leave your vessel, always take the ignition key with you.
- Consideration should be given to installing a hidden device to shut off the fuel line, or to the installation of an engine immobilizer.
- Outboard motors should be secured with a strong case-hardened steel chain padlock and hardened steel chain or some form of proprietary locking bar.
- In some cases it may be possible to cover the boat as far as the design allows and to then secure the cover.

6 Pleasure craft owners should photograph their vessel and equipment and mark it accordingly. This will assist authorities in returning equipment if it is stolen. All serial numbers on all individually identifiable parts of the boat and equipment should also be recorded and stored in a safe place on and off the vessel.

7 Where Radio Frequency Identification Tag (RFID) anti-theft systems are available, they should be given strong consideration. Not only do such systems have the potential to reduce theft risk, but they also have been shown to increase recovery rates and in some instances to reduce insurance fees.

## **8 Higher risk environments**

Pleasure craft operators should carefully scrutinize their intended route and ports of call prior to a voyage. If the voyage will include areas of heightened security concern, where terrorism and criminal activities including piracy and armed robbery are a major threat, careful consideration

should be given to possible alternative routings. Where safe and secure routes are not practicable, transits should be accomplished in the presence of other vessels, as expeditiously as possible, and prior notification made to the maritime authorities for the area whose advice should be followed. A rigorous contact schedule should be maintained, preferably via satellite or mobile telephone or similar system which cannot be used to locate the vessel via radio direction finding.

## **9 Contingency measures for security alerts**

Prior to operating in high risk environments, pleasure craft owners and operators should establish procedures for dealing with emergency navigational, health and safety, and security alerts and incidents. It is recommended that all crew be briefed fully on their roles and responsibilities prior to the voyage and that plans and procedures be rehearsed. A list of emergency actions should be posted in conspicuous places, such as near radios. Such lists should include contact information for appropriate port authority, police, coast guard and emergency services.

Owners and operators should consider designating one crew member as responsible for all aspects of the security on the vessel. Some companies now offer courses specifically tailored for blue-water yachtsmen.

## **10 Prevention of stowaways**

As outlined previously, checking or searching a pleasure craft carefully prior to getting underway is both a safety and security best practice. This is especially true in areas of heightened risk; when extra care should be taken in searching places on the vessel where a stowaway might hide, such as lazarettes, sail lockers, etc. Under these circumstances and if possible, the search should be conducted by two crew members. In the event that a stowaway is found, this will reduce the risk of the stowaway attacking or overpowering the searcher. As with finding a suspicious package or object, direct engagement is discouraged and appropriate authorities should be notified immediately.

## Appendix E

### GUIDELINES FOR MARINA, PORT AND HARBOUR AUTHORITIES<sup>12</sup>

The Guidelines are intended to provide information and best practice guidance to operators of marinas, ports, and harbours. They are not mandatory and are not intended to form the basis for a mandatory instrument.

- 1 Marina, port, and harbour operators should communicate information about:
  - the current security environment;
  - parts of the port which are subject to security conditions;
  - areas of restricted navigation;
  - descriptions of areas where there might be interaction with large commercial vessels subject to SOLAS and the ISPS Code; and
  - any local regulations produced for the guidance and direction of non-SOLAS vessels.
  
- 2 Marinas, ports and harbours not covered by a Port Facility Security Plan but located in a complex of ISPS-compliant port facilities should consider regularly reviewing their security arrangements, in cooperation with the ISPS-compliant facilities.
  
- 3 Depending on the size and complexity of the marina, port or harbour, consideration could also be given to implementing appropriate physical security measures, such as:
  - adequate illumination;
  - effective access controls;
  - passive monitoring devices;
  - segregation of visiting vessels in one particular area such that the visitors can be effectively monitored;
  - holding transient vessels arriving at night in a specific area, with vessel and personnel details recorded; and
  - installing RFID or similar systems to monitor the movements of vessels in and out of marinas, ports and harbours.
  
- 4 Marina, port and harbour facilities might consider implementing appropriate security procedures. These procedures might include:
  - training staff to be familiar with security operating procedures for their facility and for the safety of their customers and the public;
  - implementing regular security patrols, which should include:
    - walking all pontoons/docks;
    - checking that boats are moored normally;
    - being alert for any suspicious activity;
    - monitoring access gates, storage shed doors, overhead doors and fuel points; and
    - inspecting restroom facilities; and

---

<sup>12</sup> Further guidance may be found in the ILO/IMO Code of Practice on Security in Ports.

- maintaining a security log of events, which should include:
    - details of incidents and events that occurred while on patrol;
    - the identity of anyone or any organization called in for emergencies and the time/results of the call;
    - details of issues for referral to a supervisor; and
    - any information which should be noted for the awareness of the next shift personnel.
-