MEASURES TO ENHANCE MARITIME SECURITY (Item 4)
PIRACY AND ARMED ROBBERY AGAINST SHIPS (item 15)

Report of the working group

GENERAL


2. The group was attended by delegations from the following Member Governments:

   ANTIGUA AND BARBUDA     ITALY
   ARGENTINA                JAPAN
   AUSTRALIA                LIBERIA
   BAHAMAS                  MALAYSIA
   BAHRAIN                  MARSHALL ISLANDS
   BELGIUM                  NETHERLANDS
   BRAZIL                   NORWAY
   CANADA                   PANAMA
   CHINA                    PHILIPPINES
   COLOMBIA                 POLAND
   CYPRUS                   REPUBLIC OF KOREA
   DENMARK                  RUSSIAN FEDERATION
   EGYPT                     SINGAPORE
   FINLAND                   SOUTH AFRICA
   FRANCE                    SWEDEN
   GERMANY                  THAILAND
   GHANA                     TURKEY
   GREECE                    UNITED KINGDOM
   INDIA                      UNITED STATES
   ISLAMIC REPUBLIC OF IRAN
and by observers from the following non-governmental organizations in consultative status:

INTERNATIONAL CHAMBER OF SHIPPING (ICS)
INTERNATIONAL CHAMBER OF COMMERCE (ICC)
COMITÉ INTERNATIONAL RADIO-MARITIME (CIRM)
BIMCO
INTERNATIONAL ASSOCIATION OF INDEPENDENT TANKER OWNERS (INTERTANKO)
CRUISE LINES INTERNATIONAL ASSOCIATION (CLIA)
INTERNATIONAL ASSOCIATION OF DRY CARGO SHIPOWERS (INTERCARGO)
THE ROYAL INSTITUTION OF NAVAL ARCHITECTS (RINA)
INTERNATIONAL TRANSPORT WORKERS’ FEDERATION (ITF)
WORLD SHIPPING COUNCIL (WSC)
THE NAUTICAL INSTITUTE (NI)

TERMS OF REFERENCE

3 The working group was instructed, taking into account comments and decisions made in plenary, to:

With regard to agenda item 4 (Measures to enhance maritime security)

.1 further revise Guidance for the Development of National Maritime Security Legislation as set out in document MSC 95/4, taking into account document MSC 95/4/5 (ITF and IFSMA);

.2 consider documents MSC 95/4/1 (BIMCO et al), MSC 95/4/2 (Canada), MSC 95/4/3 (Canada), MSC 95/4/4 (International Electrotechnical Commission (IEC)), MSC 95/4/6 (United States) and MSC 95/INF.19 (European Commission);

.3 discuss the appropriate way forward with respect to the development of guidance on maritime cybersecurity, including the need to establish a correspondence group;

.4 if the establishment of a correspondence group is recommended, develop draft terms of reference for consideration by the Committee;

With regard to agenda item 15 (Piracy and armed robbery against ships)

.5 prepare a draft MSC circular on the Organization’s position in relation to the extent of the High Risk Area (HRA) as defined in the industry developed Best Management Practices for Protection against Somalia Based Piracy (BMP4) using the annex to document MSC 95/15/1 (Egypt) as the base;

.6 amend MSC.1/Circ.1333 and MSC.1/Circ.1334 to include provisions for a national point of contact for the Piracy and armed robbery module in GISIS as set out in document MSC 95/15/4;

.7 amend MSC.1/Circ.1406/Rev.2 in respect to accreditation of PMSC, taking into account documents MSC 95/15/3 (ISO) and MSC 95/INF.15 (Germany) and prepare draft MSC.1/Circ.1406/Rev.3; and

.8 submit a written report by Thursday, 11 June 2015.
MEASURES TO ENHANCE MARITIME SECURITY


4 As instructed, the group considered the Guidance for the Development of National Maritime Security Legislation as set out in document MSC 95/4.

5 The observer from the ITF stated that there was no compelling need for guidance on the development of national maritime security legislation and that it was doubtful whether the Organization should have been involved in adopting such guidance. In accordance with the Organization’s 2008 work plan, it was envisioned to develop high-level guidance for enabling legislation to provide an administrative structure to implement the ISPS Code. The ITF, however, believed that the proposed draft guidance went beyond creating a high-level administrative structure and was, in fact, an abbreviated and edited rewrite of the ISPS Code that did not reflect the flexibility and compromises that permit a balance between security and the needs of the human element and the continued efficiency of international shipping. The ITF also questioned the need for further guidance beyond what is in the ISPS Code as it had been in effect for more than 12 years and there was no lack of legislation in many Member States to serve as models.

6 In response to the issues raised by the observer from the ITF, the delegation of the United States stated that national maritime security legislation of States was not widely available and that while it was incumbent on Member States to also have in place an enforcement and response regime, these were not addressed by the existing IMO instruments.

7 The group agreed that the guidance was a useful tool for Member States that had not yet given full and complete effect to SOLAS chapter XI-2 and the ISPS Code but that, in its current form, caused some confusion in respect to the scope and language used therein. Several delegations proposed to use recommendatory language throughout in order to reflect the voluntary character of this guidance document.

8 The representative from the Legal Division of the Secretariat advised that, while it was true that the draft guidance was intended to be of recommendatory character, it should not use recommendatory language for mandatory provisions of IMO instruments. The group was also advised on the inclusion of non-IMO related instruments and best practices in the draft guidance.

9 The group, discussing the issue of whether to include non-IMO guidance, agreed to limit the scope of the guidance to SOLAS chapter XI-2, the ISPS Code and related IMO guidance. It was therefore agreed to consider only the relevant parts of the advice received from the Legal Division of the Secretariat on this matter.

10 A number of delegations expressed concern that the current structure of the guidance merged, in many instances, mandatory provisions of SOLAS chapter XI-2 and part A of the ISPS Code with recommendatory provisions of part B of the ISPS Code and non-IMO requirements. In order to provide clarity for States using the guidance, the group discussed whether to amend the Preamble of the guidance to explain the current approach, or to conduct a thorough review of each provision in the guidance so as to ensure that the language used in the guidance reflected whether the provision was mandatory or recommendatory.

11 The group agreed that, in order to facilitate the use of the guidance by Member States needing assistance in drafting maritime security legislation, a distinction needed to be made between those provisions that a SOLAS Contracting Government had to implement, and those that were recommendatory.
12 Recognizing that the review and amendment of the guidance to accommodate the above decision of the group would take substantial time, the group agreed that it was not feasible to finalize the guidance at this session, and discussed various options for progressing the work.

13 After some discussion, the group agreed to recommend to the Committee to re-establish the correspondence group to progress the work intersessionally.

14 After consideration, the group discussed and agreed to the draft terms of reference as set out in annex 1.

**Maritime cybersecurity**

15 The group, as instructed, considered all documents submitted on the issue of maritime cybersecurity with the aim of discussing the appropriate way forward with respect to the development of related IMO guidance.

16 In the absence of existing draft guidance on the issue and given further that the industry was currently developing guidance, the group requested the delegations representing the industry to provide details on the current status of their work.

17 The observer from BIMCO advised that the industry round-table including CLIA had made substantial progress in their guidance on cybersecurity on board ships and it was expected that this guidance would be ready to be submitted to MSC 96. On the question of who were the stakeholders to be addressed, BIMCO was of the view that all stakeholders of the supply chain would have to incorporate a maritime cybersecurity regime but that the shipping industry was currently focusing only on ships.

18 While some delegations were of the view that the Organization should commence work on maritime cybersecurity at this session, possibly limiting the work to gathering information on other organizations’ work, others were of the view that it would be more beneficial to await the outcome of the far advanced work of other organizations such as that being undertaken by industry.

19 The group reiterated that, while maritime cybersecurity was a timely and important issue, no duplication of effort should be undertaken and that it was in the interest of the Organization to support the initiative currently undertaken by the shipping industry as their work had advanced considerably.

20 On the issue of whether guidance on maritime cybersecurity, at this stage, should also include ports and terminals, the group agreed that there was a need to ensure that ports also implemented good cybersecurity risk management practices. However, the group was of the view that the Organization’s core business was ships and that it was thus important to finalize guidance for ships first.

21 The delegation of Denmark, supported by others, stated that ports were predominantly regulated under a national regime which, to a large extent, considered cybersecurity challenges in relation to the interface of a port with the hinterland.

22 The observer from BIMCO, on the question on whether ship and port guidance on cybersecurity could be merged, responded that the shipping industry would welcome any development on port cybersecurity with a view to the possibility of merging their guidance with that for ports.
Several delegations expressed the view that FAL and MSC needed to actively coordinate their work in order to avoid duplication of effort and to ensure mutual review and consistency of any work undertaken by each Committee.

The observer from BIMCO informed the group that industry planned to provide their guidelines on maritime cybersecurity on board ships to FAL 40 for information, and to MSC 96 for review.

Given the current ongoing work by industry on cybersecurity on board ships and the expected dissemination of the guidance at MSC 96 the group agreed that it would be best to await the industry submission on maritime cybersecurity on board ships before embarking on developing guidance by the Organization at this stage. Hence it was further agreed that the establishment of a correspondence group at this session was not warranted. The group also agreed to invite the Committee to urge Member States and observer organizations to collaborate on proposals for guidance on maritime cybersecurity and submit them to the next session.

**Piracy and Armed Robbery against Ships**

**Definition of the High Risk Area (HRA) as defined in the Best Management Practices for Protection against Somalia Based Piracy (BMP 4)**

The group, as instructed, considered the development of a draft circular reflecting the Committee’s position in respect to the High Risk Area (HRA) as defined in the industry developed Best Management Practices for Protection against Somalia Based Piracy (BMP4), using the annex to document MSC 95/15/1 (Egypt) as the base.

The group had an extensive discussion on this matter and the most salient points are outlined below.

The delegation of India sought clarification on whether the definition of the HRA as defined in the BMP4 needed to be further clarified, especially in respect to other existing definitions on piracy high risk areas such as from the Joint War Committee (JWC) or the International Bargaining Forum (IBF).

The observer delegations representing the shipping industry (ICS, BIMCO and INTERTANKO), in response to the query raised by India and recalling that this was a recurring question raised at various fora on this matter, suggested to provide a clarifying footnote in the draft circular making it clear that the BMP HRA was distinct from those of the JWC and IBF. However, this proposal was not agreed by the group.

A lengthy discussion took place on the issue of whether the Red Sea had experienced recent attacks of piracy and armed robbery as this was a key determining factor for the designation as a piracy high risk area. The group, while sympathetic to the Egypt position, agreed that incidents of piracy and armed robbery from various sources did not allow for the deduction that there had been no attacks in the Red Sea. Further, it was the view of the group that such an assessment was beyond the group’s knowledge and expertise and required consultation with security forces operating in the area.

In light of the above, several delegations proposed to await the outcome of the upcoming CGPCS meeting in July 2015 where this issue on the extent of the HRA was to be discussed including whether the inclusion of the Red Sea was still justified.
32 The delegation of Egypt stated that their request aimed primarily to exclude the Red Sea from the definition of the HRA but that Egypt would not object to general provisions in the BMP applicable specifically to the Red Sea. Such provisions could, for example, relate to reporting requirements or preparatory measures to be taken before entering the HRA from the Red Sea (if the Red Sea was excluded from the HRA definition).

33 After a lengthy discussion the group agreed on a draft MSC circular as set out in annex 2.

National point of contact for the Piracy and armed robbery module in GISIS

34 The group, as instructed, considered amending MSC.1/Circ.1333 and MSC.1/Circ.1334 in order to include provisions for a national point of contact for the Piracy and armed robbery module in GISIS as set out in document MSC 95/15/4.

35 The group noted that nominations of national liaison or contact points for communication of information with the Organization was not consistently termed as there were various terms used for such national contact points ("national focal point", "single point of contact" etc.). The group agreed to the term "national point of contact (NPoC)".

36 In discussing this issue, the group deliberated whether it was appropriate to amend MSC.1/Circ.1334 as the provision of an NPoC for the purpose of interfacing with the Organization would not be applicable to shipowners, ship operators, shipmasters and crew as envisaged by MSC.1/Circ.1334. The group, therefore, agreed to propose to the Committee to limit the provisions in relation to the national point of contact to MSC.1/Circ.1333.

37 After some discussion on whether the provisions in MSC.1/Circ.1333 and MSC.1/Circ.1334 should provide further detail on the role of the NPoC, the group agreed it was preferable not to limit the function of an NPoC and agreed to a generic provision as set out in annex 3.

Accreditation of Private Maritime Security Companies (PMSC)

38 The group, as instructed, amended MSC.1/Circ.1406/Rev.2 in respect to accreditation of PMSC, taking into account documents MSC 95/15/3 (ISO) and MSC 95/INF.15 (Germany) and agreed on the draft MSC.1/Circ.1406/Rev.3 as set out in annex 4.

ACTION REQUESTED OF THE COMMITTEE

39 The Committee is invited to approve the report in general and, in particular, to:

.1 note the group's discussion on the difficulties encountered in the attempt to finalize the draft Guidance for the Development of National Maritime Security Legislation (paragraphs 5 to 12);

.2 note the legal advice provided by the Legal Division of the Secretariat in relation to the draft Guidance for the Development of National Maritime Security Legislation, appended to the draft terms of reference set out in annex 1 (appendix to annex 1);
3. agree to the group’s proposal to re-establish the correspondence group intersessionally, under the coordination of the United States, in order to finalize the draft *Guidance for the Development of National Maritime Security Legislation* for submission to MSC 96 with the draft terms of reference as set out in annex 1 (paragraph 13 and annex 1);

4. note the discussion of the group related to the development of maritime cybersecurity guidance (paragraphs 15 to 24);

5. endorse the group’s recommendation to await the outcome of the industry guidance on maritime cybersecurity on board ships which is planned to be submitted to FAL 40 and MSC 96, and not to establish the correspondence group at this session (paragraph 25);

6. urge Member States and international organizations to collaborate on proposals for guidance on maritime cybersecurity and submit them to the next session (paragraph 25);

7. approve the draft MSC Circular on Best Management Practices for Protection against Somalia Based Piracy (paragraph 33 and annex 2);

8. approve the revised draft MSC.1/Circ.1333 incorporating a provision on the establishment of a National point of contact for communication of information on piracy and armed robbery to the Organization (paragraph 37 annex 3);

9. agree to the group’s recommendation not to amend MSC.1/Circ.1334 (paragraph 36); and

10. approve the revised draft MSC.1/Circ.1406/Rev.2 which includes amendments related to certification of PMSC after publication of International Standard ISO 28007 (paragraph 38 and annex 4).

***
ANNEX 1

DRAFT TERMS OF REFERENCE FOR THE CORRESPONDENCE GROUP ON GUIDANCE FOR THE DEVELOPMENT OF NATIONAL MARITIME SECURITY LEGISLATION

The correspondence group is instructed, taking into account comments, proposals and decisions made in plenary at its ninety-fifth session and documents MSC 95/4/5 (ITF and IFSMA) and MSC 95/1 (Report of the Committee), to:

.1 revise the Guidance for the Development of National Maritime Security Legislation contained in the annex to document MSC 95/4 (United States) and restructure the provisions so as to address the following issue:

.1 clearly distinguishing, either by formatting, by providing explanatory notes for each provision or by separating the guidance in different parts, between:

a. mandatory IMO provisions as contained in SOLAS chapter XI-2 and the ISPS Code,

b. IMO recommendations and guidance set out in part B of the ISPS Code and in various IMO circulars as well as the IMO Guide to Maritime Security and the ISPS Code;

.2 follow the advice provided by the Legal Division of the Secretariat on drafting the guidance in relation to issues 1 to 3 only, as set out in the appendix to this terms of reference; and

.3 submit a written report to MSC 96.

***
APPENDIX TO THE
DRAFT TERMS OF REFERENCE OF THE CORRESPONDENCE GROUP

Legal advice from the Legal Division of the Secretariat on mandatory and recommendatory language in the Guidance for the Development of National Maritime Security Legislation

The Legal Affairs Office has been asked to provide legal advice on mandatory and recommendatory language in the Guidance for the Development of National Maritime Security Legislation.

The issues in question are:

1. Whether the guidance, as a non-mandatory instrument, can provide for a mandatory language in the draft legislation;
2. Whether it is appropriate to use "shall/should" in the draft legislation;
3. How to distinguish mandatory provisions from non-mandatory;
4. Whether the guidance may contain draft provisions which go beyond the scope of SOLAS/ISPS Code, i.e. best practices.

The Legal Affairs Office's view is as follows:

1. The guidance as such is a non-mandatory instrument which will provide States in need of assistance with examples of national legislation implementing SOLAS/ISPS Code. The preamble, as well as the explanatory notes throughout the guidance, leave no doubt that the legal status of the document itself is non-binding. However, the examples of provisions which are given to illustrate how the mandatory requirements of SOLAS/ISPS Code may be implemented, do contain mandatory language ("shall" or "is"). The fact that such examples contain mandatory language does not change the legal nature of the guidance which remains a non-binding document. The use of "shall" or "is" in the sample provisions are intended to give clear guidance to States in need of assistance on how to implement mandatory requirements.

2. It is not advisable to use the wording "shall/should" throughout the guidance, including for mandatory requirements, as this will suggest that States implementing SOLAS/ISPS Code have a discretion in deciding about the binding or non-binding nature of these requirements. This may lead to an undesirable confusion. The only discretion States have is to decide whether those requirements that are recommendatory under SOLAS/ISPS Code will be mandatory in the national legislation. If they decide to make recommendatory provisions mandatory under national law, then the language of the national legislation has to be mandatory.

3. The concern arises that using mandatory language in examples of provisions that implement non-mandatory requirements may lead to a misunderstanding of the legal nature of these provisions. This concern is justified. In order to avoid any confusion it is suggested that examples of provisions which implement non-mandatory requirements (part B of ISPS Code) are distinguished from those that implement mandatory requirements. In the first place it is suggested that an appropriate explanation is contained in the preamble and in the explanatory notes. The working group may also consider using a different font type, for example italics, in order to distinguish non-mandatory requirements. This will allow all States that will use the guidance to clearly understand which provisions have a non-binding nature under international law.
4 The guidance as currently drafted contains also provisions which go beyond the scope of SOLAS/ISPS Code (i.e. enforcement provisions, offences and penalties etc.). However, it has to be noted that SOLAS Article I(b) imposes on all Contracting Governments an obligation to give "full and complete effect" to the Convention (including ISPS Code which is incorporated into the Convention under the provisions of chapter XI-2). Enforcement provisions like offences, sanctions and penalties are part of the national legislation which aim to give the Convention "full and complete effect". Therefore, the guidance may also contain examples of such provisions. These should be indicated clearly as best practices.

***
ANNEX 2

DRAFT MSC CIRCULAR

PIRACY AND ARMED ROBBERY AGAINST SHIPS IN WATERS OFF THE COAST OF SOMALIA

Best Management Practices for Protection against Somalia-based Piracy

1 The Maritime Safety Committee (the Committee), at its eighty-ninth session (11 to 20 May 2011), having, inter alia, recognized the importance of the Best Management Practices (BMP) and the recommendation therein, adopted resolution MSC.324(89) on Implementation of Best Management Practice Guidance, and expressed its general understanding of the need to keep the BMP alive, relevant, dynamic and updated. The latest version of the BMP guidance, BMP 4, was promulgated as MSC.1/Circ.1339.

2 The Committee, at its ninety-fifth session (3 to 12 June 2015), noted with appreciation that the development of the BMP guidance by the industry, and its implementation on board ships operating in the Gulf of Aden and western Indian Ocean, had been a significant factor in containment of Somalia-based piracy.

3 The Committee noted the definition of the High Risk Area (HRA) as set out in paragraph 2.4 of BMP 4, which defines the HRA, inter alia, as an area "where pirate activity and/or attacks have taken place".

4 The Committee noted further that the geographical extent of the HRA is set out in the BMP and is defined by the authors of the BMP and its signatories. The HRA as defined in the BMP is susceptible to change based on changes in the actual threat circumstances and therefore the Committee expressed sympathy for the proposal by Egypt to remove the Gulf of Suez and the Red Sea from the HRA definition in the BMP.

5 The Committee, therefore, observed that High Risk Area (HRA) may now be incorrect terminology for describing the area in which piracy attacks have not taken place but where preparatory self-protection measures are nevertheless recommended. The Committee calls on the authors of the BMP to take necessary steps to amend the coordinates of the HRA in view of excluding the above-mentioned area from the HRA definition at the earliest time, taking into consideration the threat assessment and respectfully request them to report back to MSC at its next session.

6 The Committee reiterated its strong support for the BMP and continued to stress the need for ships to continue to implement its recommended practices, taking into account the guidance provided in resolution MSC.324(89) and the Organization's current recommendations to Governments and guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships.

7 States and international organizations are invited to bring this circular to the attention of shipowners, ship operators and managers, companies, shipmasters, ship security officers and all other relevant parties.

***

* MSC.1/Circ.1333 on Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships, and MSC.1/Circ.1334 on Guidance to shipowners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships, or revisions thereto.
ANNEX 3

MSC.1/Circ.1333/Rev.1
12 June 2015

PIRACY AND ARMED ROBBERY AGAINST SHIPS
Revised Recommendations to Governments for preventing and suppressing piracy and armed robbery against ships

1 The Maritime Safety Committee, at its ninety-fifth session (3 to 12 June 2015), revised MSC.1/Circ.1333 by incorporating provisions for the establishment of a national point of contact for communication of information on piracy and armed robbery to the Organization given in the annex.

2 Member Governments, in particular those within areas identified as affected by acts of piracy and armed robbery against ships, are recommended to take any necessary action to implement, as appropriate, the recommendations given in the annex.

3 Member Governments are also recommended to bring this circular and MSC.1/Circ.1334 to the attention of all national agencies concerned with anti-piracy and anti-armed robbery activities, shipowners, ship operators, shipping companies, shipmasters and crews.

4 This circular revokes MSC.1/Circ.1333.

***

Insert the following new text after paragraph 25 in MSC.1/Circ.1333:

National point of contact for communication of information on piracy and armed robbery to the Organization

25bis Member States should communicate to the Organization the name and contact details of a national point of contact (NPoC) to interface with the Organization for piracy and armed robbery matters.
ANNEX 4

MSC.1/Circ.1406/Rev.3
12 June 2015

REVISED INTERIM RECOMMENDATIONS FOR FLAG STATES REGARDING THE USE OF PRIVATELY CONTRACTED ARMED SECURITY PERSONNEL ON BOARD SHIPS IN THE HIGH RISK AREA

1 The Maritime Safety Committee, at its eighty-ninth session (11 to 20 May 2011), approved Interim recommendations for flag States regarding the use of privately contracted armed security personnel on board ships in the High Risk Area.

2 Given the importance and urgent nature of this issue, and the need to further develop and promulgate detailed guidance and recommendations as soon as possible, the Committee approved and the Council authorized the convening of an intersessional meeting of the Maritime Security and Piracy Working Group (13 to 15 September 2011) to update the recommendations.

3 The interim recommendations were further revised by the Maritime Safety Committee at its ninetieth session (16 to 25 May 2012) to take into account minor consequential amendments arising from the development of the interim guidance to private maritime security companies set out in MSC.1/Circ.1443 on Interim guidance to private maritime security companies providing privately contracted armed security personnel on board ships in the High Risk Area.

4 The interim recommendations were again revised by the Maritime Safety Committee at its ninety-fifth session (3 to 12 June 2015), taking into account publication of International Standard ISO 28007 on certification of PMSC.

5 The Revised interim recommendations for flag States regarding the use of privately contracted armed security personnel on board ships in the High Risk Area is set out in the annex.

6 The attached revised interim recommendations should be read in conjunction with the interim guidance and recommendations set out in MSC.1/Circ.1443; MSC.1/Circ.1405/Rev.2 on Revised interim guidance to shipowners, ship operators and shipmasters on the use of privately contracted armed security personnel on board ships in the High Risk Area; and MSC.1/Circ.1408/Rev.1 on Revised interim recommendations for port and coastal States regarding the use of privately contracted armed security personnel on board ships in the High Risk Area, and the information provided in MSC-FAL.1/Circ.2 on Questionnaire on information on port and coastal State requirements related to privately contracted armed security personnel on board ships, as well as the other recommendations and guidance developed by the Organization for preventing and suppressing piracy and armed robbery against ships.

---

1 High Risk Area: an area as defined in the Best Management Practices for Protection against Somalia-based Piracy (MSC.1/Circ.1339), unless otherwise defined by the flag State.

2 As they may be revised.
7 Member Governments are urged to bring this circular to the attention of all national agencies concerned with anti-piracy activities, shipowners, ship operators, shipping companies, shipmasters and crews.

8 Member Governments are also urged to take any necessary action to implement, as appropriate, the revised interim recommendations given in the annex.

9 Member Governments, international organizations and non-governmental organizations with consultative status are invited to bring to the attention of the Committee, at the earliest opportunity, the results of the experience gained from the use of the revised interim recommendations so as to assist the Committee in deciding on any action to be taken.

10 MSC.1/Circ.1406/Rev.2 is hereby revoked.

***

In the annex to the circular, replace existing paragraph 5 by the following text:

5 Flag States should have in place a policy on whether or not the use of PCASP will be authorized and, if so, under which conditions. In developing such a policy, flag States are encouraged to take into account the following recommendations:

.1 As a first step, consider whether the use of PCASP:

.1 would be permitted under the national legislation of the flag State;

.2 would be an appropriate measure under some circumstances to augment the security arrangements put in place, in accordance with related instruments and guidelines developed and promulgated by the Organization including the industry-developed best management practices, on ships flying its flag when operating in the High Risk Area; and

.2 As a second step, if the use of PCASP is determined to be an appropriate and lawful measure, establish a policy which may include, inter alia:

.1 the minimum criteria or minimum requirements with which PCASP should comply, taking into account the relevant aspects of the guidance set out in MSC.1/Circ.1405/Rev.2 on Revised interim guidance to shipowners, ship operators, and shipmasters on the use of privately contracted armed security personnel on board ships in the High Risk Area;
.2 ensuring that PMSC employing PCASP on board ships hold valid accredited certification to ISO 28007-1:2015 (Ships and marine technology – Guidelines for Private Maritime Security Companies (PMSC) providing privately contracted armed security personnel (PCASP) on board ships) or meet applicable national requirements;

.3 a process for authorizing the use of PCASP which have been found to meet minimum requirements for ships flying its flag;

.4 a process by which shipowners, ship operators or shipping companies may be authorized to use PCASP;

.5 the terms and conditions under which the authorization is granted and the accountability for compliance associated with that authorization;

.6 references to any directly applicable national legislation pertaining to the carriage and use of firearms by PCASP, the category assigned to PCASP, and the relationship of PCASP with the Master while on board;

.7 reporting and record-keeping requirements; and

.3 Provide information to the Organization on the use of PCASP for circulation to Member States.