澳門特別行政區

行 政 長 官 辦 公 室

第 22/2015 號行政長官公告

中華人民共和國於一九九九年十二月十三日以照會通知聯合國秘書長，經修訂的《1974年國際海上人命安全公約》自一九九九年十二月二十日起適用於澳門特別行政區；

公約締約政府會議於二零零二年十二月十二日透過決議2通過了《國際船舶和港口設施保安規則》，該規則自二零零四年七月一日起適用於澳門特別行政區；

基於此，行政長官根據澳門特別行政區第3/1999號法律第六條第一款的規定，命令公佈包含上指規則的會議決議2的中文及英文文本。

二零一五年四月九日發佈。

行政長官　崔世安

REGIÃO ADMINISTRATIVA ESPECIAL DE MACAU

GABINETE DO CHEFE DO EXECUTIVO

Aviso do Chefe do Executivo n.º 22/2015

Considerando que a República Popular da China, por nota datada de 13 de Dezembro de 1999, notificou o Secretário-Geral das Nações Unidas sobre a aplicação da Convenção Internacional para a Salvaguarda da Vida Humana no Mar de 1974, tal como emendada, na Região Administrativa Especial de Macau a partir de 20 de Dezembro de 1999;

Considerando igualmente que, em 12 de Dezembro de 2002, a Conferência dos Governos Contratantes da Convenção, através da resolução n.º 2, adoptou o Código Internacional para a Protecção dos Navios e das Instalações Portuárias, e que tal Código é aplicável na Região Administrativa Especial de Macau, a partir de 1 de Julho de 2004;

O Chefe do Executivo manda publicar, nos termos do n.º 1 do artigo 6.º da Lei n.º 3/1999 da Região Administrativa Especial de Macau, a resolução n.º 2 da Conferência, que contém o referido Código, nos seus textos em línguas chinesa e inglesa.

Promulgado em 9 de Abril de 2015.

O Chefe do Executivo, *Chui Sai On*.

《1974 年國際海上人命安全公約》締約政府會議的決議 2

（2002 年 12 月 12 日通過）

通過《國際船舶和港口設施保安規則》

會議，

通過了經修正的《1974 年國際海上人命安全公約》（此後稱為“本公約”）有關強化海上安全和保安的特別措施的修正案，

考慮到本公約新的第 XI-2 章提及《國際船舶和港口設施保安（ISPS）規則》並要求船舶、公司和港口設施根據《ISPS 規則》的規定符合《國際船舶和港口設施保安（ISPS）規則》第 A 部分的有關要求，

認為締約政府對該章的實施會大大有助於強化海上安全和保安和維護船上和岸上的安全和保安，

審議了國際海事組織（此後稱為“本組織”）海上安全委員會第七十五和七十六次會議準備的、供本會議審議和通過的《國際船舶和港口設施保安規則》草案，

1. **通過**《國際船舶和港口設施保安規則》（此後稱為“本規則”），其條文載於本決議的附件中；

2. **請**公約的締約政府注意：本規則將在本公約新的第 XI-2 章生效後於 2004 年 7 月 1 日生效；

3. **要求**海上安全委員會對本規則不斷作出檢查並視情予以修正；

4. **要求**本組織秘書長將本決議及附件中所載的本規則的條文的核證無誤副本發給本公約的所有締約政府；

5. **還要求**秘書長將本決議及其附件的副本發給非本公約締約政府的本組織的所有會員。

附件

國際船舶和港口設施保安規則

序言

1 2002 年 12 月在倫敦舉行的海上保安外交會議通過了《1974 年國際海上人命安全公約》的新規定及本規則，以強化海上保安。這些新要求構成了船舶和港口設施能夠合作偵查和阻止威脅海上運輸保安行為的國際框架。

2 在 2001 年 9 月 11 日的悲慘事件後，國際海事組織（本組織）大會第 22 次會議於 2001 年 11 月一致同意制定有關船舶和港口設施保安的新措施，供 2002 年 12 月的《1974 年國際海上人命安全公約》締約政府會議（即海上保安外交會議）通過。本組織的海上安全委員會（MSC）被責成在各會員國、國際組織和享有本組織諮詢地位的非政府組織的提案基礎上籌備該外交會議。

3 也於 2001 年 11 月舉行的 MSC 第一次特別會議，為加速制定和通過適當的保安措施，設立了 MSC 休會期間海上保安工作組。MSC 休會期間海上保安工作組第一次會議於 2002 年 2 月舉行，其討論結果被報告給 2002 年 5 月的 MSC 第七十五次會議並由該次會議作出審議；在其時設立了一個特設工作組對提交的提案作出了進一步的制定。MSC 第七十五次會議審議了該工作組的報告並建議由 2002 年 9 月舉行的另一次 MSC 休會期間工作組會議作進一步工作。MSC 第七十六次會議審議了 MSC 休會期間工作組的 2002 年 9 月會議的成果和

與在外交會議前不久的2002年12月的該委員會第七十六次會議一起舉行的 MSC 工作組的進一步工作並同意了由外交會議審議的提議條文的最後文本。

4 外交會議（2002年12月9日至13日）還通過了《1974年國際海上人命安全公約》(《SOLAS 74》）有關加速實施安裝自動識別系統要求的現有規定的修正案和通過了《SOLAS 74》第 XI-1 章有關標誌船舶識別號和攜帶連續摘要記錄的新規則。外交會議還通過了一些會議決議，包括有關本規則的實施和修訂、技術合作和與國際勞工組織和世界貿易組織的合作工作的決議。會議認識到，在這兩個組織的工作完成後可能需要對有關海上保安的若干規定作出檢查和修正。

5 《SOLAS 74》第 XI-2 章的規定和本規則適用於船舶和港口設施。同意將《SOLAS 74》擴大到包括港口設施是因為《SOLAS 74》提供了確保必要保安措施能得到迅速生效和實施的最快手段。但還同意：有關港口設施的規定應僅與船/港界面相關。港口保安的更廣泛問題將是國際海事組織與國際勞工組織的新的聯合工作的主題。又同意這些規定不應擴大到對襲擊的實際反應或此種襲擊後的任何必要清理活動。

6 在起草該規定時，注意到要確保與經修正的《1978年國際船員培訓、發證和值班標準公約》、《國際安全管理（ISM）規則》和一致的檢驗和發證制度的規定的兼容。

7 這些規定代表了國際海事業對海上運輸段的保安問題的處理方法的重大改變。人們認識到它們可能對若干締約政府造成重大的額外負擔。人們充分認識到幫助各締約政府實施這些規定的技術合作的重要性。

8 這些規定的實施將需要包括船舶人員、港口人員、旅客、貨主、船舶和港口的管理人員和負有保安責任的國家和地方當局人員在內的所有涉及或使用船舶和港口設施的人員間的繼續有效合作和理解。現有的做法和程序如不提供適當的保安水平，則應被檢查和更改。為了強化海上保安，航運和港口業以及國家和地方當局必須承擔額外責任。

9 在實施《SOLAS 74》第 XI-2 章和本規則第 A 部分的保安規定時，應計及本規則第 B 部分中的指導。但人們認識到該指導的適用範圍可視港口設施和船舶及其貿易和/或貨物的性質而有不同。

10 對本規則的任何規定的解釋和應用均不得違背對各國際文件特別是包括“國際勞工組織工作基本原則和權利宣言”和海上和港口工人的國際標準在內的有關海上工作者和難民的此種文件中規定的基本權利和自由的充分尊重。

11 認識到經修正的《1965 年便利海上運輸公約》規定：當載有外國船員的船舶在港口中時，只要完成了船舶抵達手續且公共當局沒有理由因公眾健康、公眾安全或公眾秩序的原因拒絕允許上岸，公共當局應允許外國船員上岸。締約政府在核准船舶和港口保安計劃時應充分認識到如下事實：船舶人員在船上生活和工作，因此需要岸登假和使用岸上的船員福利設施，包括醫療。

第 A 部分

經修正的《1974 年國際海上人命安全公約》附件

第 XI-2 章的規定的強制性要求

1 總則

1.1 序言

《國際船舶和港口設施保安規則》的本部分載有經修正的《1974 年國際海上人命安全規則》第 XI-2 章中提及的強制性規定。

1.2 目標

本規則的目標是：

.1 建立締約政府、政府機構、地方管理機構和航運和港口業合作偵查保安威脅並採取預防措施防範影響國際貿易中使用的船舶和港口設施的保安事件的國際框架；

.2 確定締約政府、政府機構、地方管理機構和航運和港口業在國家和國際水平上確保海上保安的各自任務和責任；

.3 確保及早和有效地收集和交換保安信息；

.4 提供保安評定方法，使計劃和對改變的保安級別作出反應的程序就位；

.5 確保對有就位的適當和適度保安措施的信心。

1.3 功能要求

為實現其目標，本規則載有一些功能要求。這些要求包括但不限於：

.1 收集和評定有關保安威脅的信息，與有關締約政府交換此種信息；

.2 要求維護船舶和港口的通信規約；

.3 防止擅自進入船舶、港口設施及其禁區；

.4 防止將未允許的武器、點燃裝置或爆炸品帶入船舶和港口設施；

.5 提供對保安威脅或保安事件作出反應的報警裝置；

.6 要求以保安評定為基礎的船舶和港口設施保安計劃；和

.7 要求旨在確保熟習保守計劃和程序的培訓、操練和演習。

2 定義

2.1 除另有明文規定者外，就本部分而言：

.1 *本公約*係指經修正的《1974 年國際海上人命安全公約》。

.2 *條*係指本公約的某一條。

.3 *章*係指本公約的某一章。

.4 *船舶保安計劃*係指為確保應用旨在保護船上人員、貨物、貨物運輸單元、船舶物料或船舶免受保安事件風險危害的船上措施而制定的計劃。

.5 *港口設施保安計劃*係指為確保應用旨在保護港口設施和港口設施內的船舶、人員、貨物、貨物運輸單元和船舶物料免受保安事件風險的危害的措施而制定的計劃。

.6 *船舶保安官員*係指對船長負責、被公司指定負責包括實施和保持船舶保安計劃在內的船舶保安和與公司保安官員和港口設施保安官員聯絡的船上人員。

.7 *公司保安官員*係指公司指定的確保進行船舶保安評定、制定船舶保安計劃、將其提交供核准並在此後予以實施和保持及與港口設施保安官員和船舶保安官員聯絡的人員。

.8 *港口設施保安官員*係指被指定負責制定、實施、修改和保持港口設施保安計劃和負責與船舶保安官員和公司保安官員聯絡的人員。

.9 *1 級保安*係指在任何時候均應保持最低適當保護性保安措施的級別。

.10 *2 級保安*係指由於更大的保安事件風險在某一期間內應保持適當額外保護性保安措施的級別。

.11 *3 級保安*係指在雖不能確定具體目標但保安事件是可能或即將發生的有限期間內應保持進一步的具體保護性保安措施的級別。

2.2 “船舶”一詞在本規則中使用時包括第 XI-2/1 條中規定的移動式近海鑽井裝置和高速船。

2.3 “締約政府”一詞在第 14 至 18 節中使用時，如涉及對港口設施的任何提及，則包括對“指定當局”的提及。

2.4 在本部分中未作其他定義的術語應與第 I 和 XI-2 章中給予的定義具有相同意思。

3 適用範圍

3.1 本規則適用於：

.1 從事國際航行的下列船型：

.1 客船，包括高速客船；

.2 等於和大於 500 總噸的貨船，包括高速船；和

.3 移動式近海鑽井裝置；和

.2 為從事國際航行的此種船舶服務的港口設施。

3.2 雖有 3.1.2 節的規定，締約政府應決定本規則的本部分對其領土內的雖主要由非從事國際航行的船舶使用但偶爾需為從事國際航行的抵、離船舶服務的那些港口設施的適用範圍。

3.2.1 締約政府應根據按本規則的本部分進行的港口設施保安評定作出 3.2 節規定的決定。

3.2.2 締約政府根據 3.2 節作出的任何規定均不應損害第 XI-2 章或本規則的本部分要達到的保安水平。

3.3 本規則不適用於軍艦、海軍輔助船或由締約政府擁有或運營且僅用於政府非商業服務的其他船舶。

3.4 本部分第 5 至 13 節和第 19 節適用於第 XI-2/4 條中規定的公司和船舶。

3.5 本部分第 5 節和第 14 至 18 節適用於第 XI-2/10 條規定的港口設施。

3.6 本規則中的任何規定均不損害國際法規定的國家權利和義務。

4 締約政府的責任

4.1 以 XI-2/3 和 XI-2/7 條的規定為準，締約政府應確定保安級別和提供防止保安事件的指導。保安級別越高則表明發生保安事件的可能性越大。在確定適當保安級別時應考慮的因素包括：

.1 威脅信息的可信程度；

.2 威脅信息的核實程度；

.3 威脅信息的具體和緊迫程度；和

.4 此種保安事件的潛在後果。

4.2 締約政府在確定 3 級保安時，如必要，應發佈適當指示並向可能受到影響的船舶和港口提供保安信息。

4.3 締約政府可委託經認可的保安組織履行第 XI-2 和本規則的本部分對某規定的若干職責，但下列者除外：

.1 確定適當的保安級別；

.2 核准港口設施保安評定及經核准的評定的此後修正案；

.3 確定需要指定港口設施保安官員的港口設施；

.4 核准港口設施保安計劃及經核准的計劃的此後修正案；

.5 按第 XI-2/9 條實施控制和符合措施；和

.6 制定對“保安聲明”的要求。

4.4 締約政府應在其認為適當的範圍內檢驗經其核准的或，對於船舶，經其代表核准的船舶保安計劃或港口設施保安計劃或此種計劃的修正案的有效性。

5 保安聲明

5.1 締約政府應通過評定船/港界面或船對船活動對人員、財產或環境的風險來確定何時需要“保安聲明”。

5.2 在下列任一情況下船舶可要求填寫“保安聲明”：

.1 船舶的保安級別高於其所界面的港口設施或另一船舶的保安級別；

.2 對若干國際航行或從事此種航行的具體船舶，在締約政府間有“保安聲明”協議；

.3 有過涉及船舶或港口設施的保安威脅或保安事件；

.4 船舶在不要求備有或實施經核准的港口設施保安計劃的港口中；或

.5 船舶在與不要求備有或實施經核准的船舶保安計劃的另一船舶進行船對船活動。

5.3 適用的港口設施或船舶應對按本節規定提出的填寫“保安聲明”的要求作出確認。

5.4 “保安聲明”應由下列者填寫：

.1 船長或代表該船的船舶保安官員；和，如適當，

.2 港口設施保安官員或，如締約政府另有決定，代表該港口設施的負責岸側保安的任何其他機構。

5.5 “保安聲明”應陳述港口設施和船舶（或船舶間）分擔的保安要求並應說明各方的責任。

5.6 締約政府應記及第 XI-2/9.2.3 條的規定，對其領土內的港口設施保留“保安聲明”的最低期限作出規定。

5.7 各主管機關應記及第 XI-2/9.2.3 條的規定，對有權懸掛其國旗的船舶保留“保安聲明”的最低期限作出規定。

6 公司的義務

6.1 公司應確保船舶保安計劃載有強調船長權威的明確陳述。公司應在船舶保安計劃中規定：船長在作出有關船舶安全和保安的決定和在必要時要求公司或任何締約政府提供援助方面具有最高的權威和責任。

6.2 公司應確保公司保安官員、船長和船舶保安官員得到履行其第 XI-2 章和本規則的本部分規定的職責和責任的必要支持。

7 船舶保安

7.1 要求船舶按下列規定對締約政府確定保安級別採取行動。

7.2 1 級保安：應計及本規則第 B 部分中的指導，通過適當措施，在所有船舶上開展下列活動，以查明保安事件並對其採取預防措施。

.1 確保履行所有的船舶保安職責；

.2 控制對船舶的通入；

.3 控制人員及其個人物品的上船；

.4 監視禁區，確保只有經允許的人員進入；

.5 監視甲板區域和船舶周圍區域；

.6 監控貨物和船舶物料的裝卸；和

.7 確保保安通信的隨時可用。

7.3 2 級保安：應計及本規則第 B 部分中的指導，對 7.2 節中詳述的每活動實施在船舶保安計劃中規定的額外保護措施。

7.4 3 級保安：應計及本規則第 B 部分中的指導，對 7.2 節中詳述的第一活動實施船舶保安計劃中規定的進一步的具體保護措施。

7.5 每當主管機關確定 2 級或 3 級保安時，船舶應對有關改變保安級別的指示作出收迄通知。

7.6 在進入確定了 2 級或 3 級保安的某一締約當事國領土內的港口前或在此種港口內時，船舶應對該指示作出收迄通知並應向港口設施保安官員確認對船舶保安計劃中和，對於 3 級保安，在確定 3 級保安的締約政府發出的指示中詳述的適當措施和程序的實施啟動。船舶應報告任何實施困難。在此種情況下，港口設施保安官員和船舶保安官員應進行聯絡並協調適當行動。

7.7 如主管機關要求船舶確定或船舶已處於比對其意圖進入的港口或其已在港口所確定者更高的保安級別，則船舶應及時向港口設施

在其領土內的締約政府的主管當局和港口設施保安官員通報此種情況。

7.7.1 在此種情況下，船舶保安官員應與港口設施保安官員聯絡並在必要時協調適當行動。

7.8 要求有權懸掛其國旗的船舶在另一締約政府的港口中確定 2 級或 3 級保安的主管機關應及時向該締約政府作出通知。

7.9 在締約政府確定保安級別並確保向在其領海中營運或已作出意圖進入其領海的通知的船舶提供保安級別信息時，應建議此種船舶保持警惕並將其得悉的可能影響該區域的海上保安的任何信息立即報告其主管機關和任何附近的沿海國。

7.9.1 在向此種船舶通報適當的保安級別時，締約政府還應計及本規則第 B 部分中的指導，向這些船舶通報它們應採取的任何保安措施和，如適當，該締約政府已採取的防止威脅的措施。

8 船舶保安評定

8.1 船舶保安評定是制定和更新船舶保安計劃工作的必要和不可缺少的部分。

8.2 公司保安官員應計及本規則第 B 部分中的指導，確保船舶保安評定係由對船舶保安評估具有適當技能的人員按本節進行。

8.3 以第 9.2.1 節的規定為準，經認可的保安組織可進行特定船舶的船舶保安評定。

8.4 船舶保安評定應包括現場保安檢驗和至少下列要素：

.1 指明現有的保安措施、程序和作業；

.2 指明和評估應重點保護的關鍵船上作業；

.3 指明對關鍵船上作業的可能威脅及其發生的可能性，以制定保安措施及其優先順序；和

.4 指明基礎設施、政策和程序中的弱點，包括人的因素。

8.5 公司應將船舶保安評定制成文件，予以檢查、接受和保存。

9 船舶保安計劃

9.1 每一船舶應在船上攜帶經主管機關核准的船舶保安計劃。計劃應對本規則的本部分中定義的三個保安級別作出準備。

9.1.1 以第 9.2.1 節的規定為準，經認可的保安組織可制定特定船舶的船舶保安計劃。

9.2 主管機關可將對船舶保安計劃或對以前核准的計劃的修正案的檢查和核准委託給經認可的保安組織。

9.2.1 在此種情況下，檢查或核准特定船舶的船舶保安計劃或其修正案的經認可的保安組織不應參與被檢查的船舶保安評定、船舶保安計劃或修正案的制定工作。

9.3 在提交船舶保安計劃或以前核准的計劃的修正案供核准時，應附有作為制定該計劃或修正案的基礎的保安評定。

9.4 此種計劃在制定時應計及本規則第 B 部分中的指導並以船舶的一種或多種工作語文寫成。如果使用的語文不是英文、法文或西班牙文，則應包括其中一種語文的譯文。該計劃應至少陳述以下事項：

.1 旨在防止武器或用以危害人員、船舶和港口和未允許裝載的任何其他危險物質和裝置被帶到船上的措施；

.2 指明禁區和防止擅自進入禁區的措施；

.3 防止擅自進入船舶的措施；

.4 對保安威脅和破壞保安行為的反應程序，包括保持船舶或船/港界面的關鍵作業的措施；

.5 對締約政府在3級保安下可能發出的任何保安指示的反應程序；

.6 保安威脅或破壞保安行為的評估程序；

.7 負有保安責任的船上人員或其他船上人員在保安方面的職責；

.8 審核保安活動的程序；

.9 與計劃相關的培訓、操練和演習的程序；

.10 與港口設施保安活動界面的程序；

.11 定期檢查計劃和更新計劃的程序；

.12 報告保安事件的程序；

.13 船舶保安官員的識別；

.14 公司保安官員的識別，包括24小時聯絡的詳細資料；

.15 確保對船上配備的任何保安設備作出檢查、測試、校準和保養的程序；

.16 測試或校準船上配備的任何保安設備的頻度；

.17 指明配有船舶保安警戒啓動點的位置；和

.18 有關使用船舶保安警戒系統的程序、說明書和指導，包括測試、啓動、解除啓動、重新設定和制限假警戒。

9.4.1 對計劃中規定的保安活動進行內部審核或對其實踐作出評估的人員應獨立於被審核的活動，除非由於公司或船舶的規模和性質這樣做是不可行的。

9.5 主管機關應確定經核准的船舶保安計劃或在經核准的計劃中規定的任何保安設備的哪些更改不應被實施，除非該計劃的有關修正案經主管機關作出核准。任何此種更改應至少與第 XI-2 章和本規則的本部分中規定的措施同等有效。

9.5.1 經主管機關按 9.5 節特別核准的船舶保安計劃或保安設備的更改的性質，應制成文件並在文件中指出指明此種核准。該核准應在船上攜帶並與“國際船舶保安證書”（或“臨時國際船舶保安證書”）一起展示。如果這些更改是暫時的，則在恢復了原先的經核准的措施或設備後無需在船上保留該文件。

9.6 該計劃可以電子方式保存。在此種情況下，它應由旨在防止擅自刪除、銷毀或修改的程序作出保護。

9.7 應防止擅自查閱或洩露計劃。

9.8 船舶保安計劃不應受到實施第 XI-2/9 條規定的控制和符合措施的締約政府正式授權官員的檢查，但 9.8.1 節中的規定的情況除外。

9.8.1 如果締約政府正式授權官員有明確認為船舶不符合第 XI-2 章或本規則第 A 部分的要求，且核查或糾正不符合狀況的唯一措施是檢查船舶保安計劃的有關要求，則僅在有關船舶的締約政府或船長同意時方可例外允許有限查閱該計劃中與不符有關的特定部分。但計劃中與本規則的本部分的 9.4 節的.2、.4、.5、.7、.15、.17 和.18 小節有關的規定被視為是機密信息，除非各有關締約政府有其他協議，否則不能受到檢查。

10 記錄

10.1 船舶保安計劃中所述的如下活動的記錄應計及第 XI-2/9.2.3 條的規定，在主管機關規定的最低期限內在船上保留：

.1 培訓、操練和演習；

.2 保安威脅和保安事件；

.3 破壞保安行為；

.4 保安級別的更改；

.5 與船舶直接保安（如對船舶或對船舶正在或曾在的港口設施的具體威脅）相關的通信；

.6 對保安活動的內部審核和檢查；

.7 對船舶保安評定的定期檢查；

.8 對船舶保安計劃的定期檢查；

.9 對該計劃的任何修正案的實施；

.10 船上配備的任何保安設備的保養、校準和測試，包括船舶保安警戒系統的測試。

10.2 記錄應以船舶的一種或多種工作語文填寫。如果使用的語文不是英語、法語或西班牙語，則應包括其中一種語文的譯文。

10.3 記錄可以電子方式保存。在此種情況下，它們應由旨在防止擅自刪除、銷毀或修改的程序作出保護。

10.4 應防止擅自查閱或洩露記錄。

11 公司保安官員

11.1 公司應任命一位公司保安官員。視公司經營的船舶數量和類型而定，被任命為公司保安官員的人員可擔任一艘或多艘船舶的公司保安官員，但應指明該人員負責的船舶。視公司經營的船舶數量和類型而定，公司可任命多個人員為公司保安官員，但應指明每一人員負責的船舶。

11.2 除本規則的本部分在其他地方規定者外，公司保安官員的職責和責任應包括但不限於：

.1 使用適當的保安評定和其他有關信息提出船舶可能遇到的威脅水平；

.2 確保作出保安評定；

.3 確保船舶保安計劃的制定、提交供核准和此後的實施和保持；

.4 確保視情對船舶保安計劃作出修改，糾正缺陷並滿足各個船舶的保安要求；

.5 安排保安活動的內部審核和檢查；

.6 安排主管機關或經認可的保安組織對船舶的初次和此後核查；

.7 確保及時研究和處理在內部審核、定期檢查、保安檢查和符合核查期間查明的缺陷和不符；

.8 提高保安意識和警惕；

.9 確保對負責船舶保安的人員的適當培訓；

.10 確保船舶保安官員與有關港口設施保安官員之間的有效通信和合作；

.11 確保保安要求和安全要求之間的一致；

.12 確保如使用姊妹船或艦隊保安計劃，則每一船舶的計劃應準確反映出具體船舶的信息；和

.13 確保經核准的特定船舶或船組的任何替代或等效安排得到實施和保持。

12 船舶保安官員

12.1 在每一船舶上應任命一位船舶保安官員。

12.2 除本規則的本部分在其他地方規定者外，船舶保安官員的職責和責任應包括但不限於：

.1 對船舶進行定期保安檢查，確保適當的保安措施得到保持；

.2 保持和監督船舶保安計劃（包括該計劃的任何修正案）的實施；

.3 與其他船上人員和有關的港口設施保安官員協調貨物和船舶物料裝卸的保安問題；

.4 建議對船舶保安計劃的修改；

.5 向船舶保安官員報告在內部審核、定期檢查、保安檢查和符合核查期間查明的任何缺陷和不符及實施任何糾正行動；

.6 提高船上的保安意識和警惕；

.7 確保視情向船上人員提供了適當培訓；

.8 報告所有的保安事件；

.9 與公司保安官員和有關的港口設施保安官員協調船舶保安計劃的實施；和

.10 確保保安設備（如果有的話）得到適當的操作、測試、校準和保養。

13 船舶保安培訓、操練和演習

13.1 計及本規則第 B 部分中的指導，公司保安官員和適當的岸上人員應具有知識和接受過培訓。

13.2 計及本規則第 B 部分中的指導，船舶保安官員應具有知識和接受過培訓。

13.3 計及本規則第 B 部分中的指導，負有具體保安職責和責任的船上人員應了解船舶保安計劃中陳述的其船舶保安責任並應具有足夠的知識和能力履行其被指定的職責。

13.4 計及本規則第 B 部分中的指導，為確保船舶保安計劃的有效實施，應計及船型、人員變化、到訪的港口設施和其他有關情況，每隔適當時間進行操練。

13.5 計及本規則第 B 部分中的指導，公司保安官員應通過每隔適當時間參加演習，確保船舶保安計劃的有效協調和實施。

14 港口設施保安

14.1 要求港口設施按它在其領土中的締約政府確定的保安級別行動。港口設施中採用的保安措施和程序應對旅客、船舶、船舶人員和訪問者、貨物和業務造成最小的干擾或延誤。

14.2 在 1 級保安時，應計及本規則第 B 部分中的指導，通過適當措施在所有港口中進行下列活動來確定和採取防止保安事件的措施：

.1 確保履行所有的港口設施保安職責；

.2 控制港口設施的通入；

.3 監視港口設施，包括錨泊和靠泊區域；

.4 監視禁區，確保只有經允許的人員進入；

.5 監控貨物的裝卸；

.6 監控船舶物料的裝卸；和

.7 確保保安通信的隨時進行。

14.3 在 2 級保安時，應計及本規則第 B 部分中的指導，對 14.2 節中詳述的每一活動實施港口設施保安計劃中規定的額外保護措施。

14.4 在 3 級保安時，應計及本規則第 B 部分中的指導，對 14.2 節中詳述的每一活動實施港口設施保安計劃中規定的進一步的具體保護措施。

14.4.1 此外，在 3 級保安時，要求港口設施對港口設施在其領土中的締約政府發出的任何保安指示作出反應和實施。

14.5 當港口設施保安官員得悉船舶在符合第 XI-2 章或本部分的要求方面或在實施船舶保安計劃中詳述的適當措施和程序方面遇到困難時，和對於 3 級保安，在港口設施在其領土內的締約政府發出任何保安指示後，港口設施保安官員和船舶保安官員應進行聯絡並協調適當行動。

14.6 當港口設施保安官員得悉船舶的保安級別高於港口設施的保安級別時，港口設施保安官員應將此事報告主管當局，如必要，應與船舶保安官員聯絡並協調適當行動。

15 港口設施保安評定

15.1 港口設施保安評定是制定和更新港口設施保安計劃工作的必要和不可缺少的部分。

15.2 港口設施保安評定應由港口設施在其領土內的締約政府進行。締約政府可授權經認可的保安組織進行其領土內特定港口設施的港口設施保安評定。

15.2.1 在經認可的保安組織進行了港口設施評定後，港口設施在其領土內的締約政府，為符合本節，應對保安評定作出檢查和核准。

15.3 計及本規則第 B 部分中的指導，進行保安評定的人員應具有按照本節對港口設施保安作出評定的適當技能。

15.4 應計及改變的威脅和/或港口設施的小改變對港口設施安全評定作出定期檢查和更新；在港設施有重大改變發生時，總應作出檢查和更新。

15.5 港口設施安全評定應至少包括以下要素：

.1 對要重點保護的主要資產和基礎設施的確定和評估；

.2 確定對資產和基礎設施的可能威脅及其發生的可能性，以制定保安措施和確定其優先順序；

.3 對對策和程序改變及其對減少弱點的有效程度的確定、選擇和優先順序化；和

.4 確定基礎設施、政策和程序的弱點，包括人的因素。

15.6 如果多個港口設施的經營人、位置、運行、設備和設計是相似的，則締約政府可允許某一港口設施保安評定包括多個此種港口設施。允許此種安排的任何締約政府應將其細節通知本組織。

15.7 在完成港口設施保安評定後，應準備一份報告。報告應由評定方法摘要、對評定時發現的每一弱點的陳述以及對可用以處理每一弱點的對策的陳述構成。應防止擅自查閱或洩露報告。

16 港口設施保安計劃

16.1 應在每一港口設施的港口設施保安評定的基礎上制定和保持適合於該船/港界面的港口設施保安計劃。該計劃應對本規則的本部分中規定的三個保安級別作出準備。

16.1.1 以 16.2 節的規定準，經認可的保安組織可準備某一特定港口設施的港口設施保安計劃。

16.2 港口設施保安計劃應由該港口設施在其領土內的締約政府核准。

16.3 此種計劃在制定時應計及本規則第 B 部分中的指導並應使用該港口設施的工作語文寫成。該計劃應至少闡述下列事項：

.1 旨在防止武器或用以危害人員、船舶或港口和未允許裝載的任何其他危險物質和裝置進入港口設施或船上的措施；

.2 旨在防止擅自進入港口設施、在設施中繫泊的船舶和設施禁區的措施；

.3 對保安威脅或破壞保安行為的反應程序，包括對保持港口設施或船/港界面的關鍵作業的準備；

.4 對港口設施在其領土內的締約政府在 3 級保安時可能發出的任何保安指示的反應程序；

.5 在保安威脅或破壞保安行為時的撤離程序；

.6 負有保安責任的港口設施人員和其他設施人員在保安方面的職責；

.7 與船舶保安活動界面的程序；

.8 定期檢查計劃和更新計劃的程序；

.9 報告保安事件的程序；

.10 港口設施保安官員的識別，包括 24 小時的聯絡細節；

.11 確保計劃中所載信息的保安的措施；

.12 旨在確保港口設施中的貨物和貨物裝卸的有效保安的措施；

.13 審核港口設施保安計劃的程序；

.14 在港內船舶的保安警戒系統被啟動時的反應程序；和

.15 便利船舶人員的登岸假或人員變動和訪問者（包括海員的福利和勞工組織的代表）進入船舶的程序。

16.4 對計劃中規定的保安活動進行內部審核或對其實施作出評估的人員應獨立於被審核的活動，除非由於港口設施的規模和性質這樣做是不可行的。

16.5 港口設施保安計劃可與港口保安計劃或與任何其他港口應急計劃結合在一起或為其組成部分。

16.6 港口設施在其領土內的締約政府應確定港口設施保安計劃的哪些改變不應被實施，除非該計劃的有關修正案由其作出核准。

16.7 該計劃可以電子方式保存。在此種情況下，它應由旨在防止擅自刪除、銷毀或修改的程序加以保護。

16.8 應防止擅自查閱或洩露計劃。

16.9 如果多個港口設施的經營人、位置、運行、設備和設計是相似的，則締約政府可允許某一港口設施保安計劃包括多個此種港口設施。允許此種替代安排的任何締約政府應將其細節通知本組織。

17 港口設施保安官員

17.1 應為每一港口設施任命一位港口設施保安官員。可任命一位人員擔任一個或多個港口設施的港口設施保安官員。

17.2 除本規則的本部分的其他地方規定者外，港口設施保安官員的職責和責任應包括但不限於：

.1 計及有關的港口設施保安評定對港口設施進行初次全面保安檢驗；

.2 確保港口設施保安計劃的制定和保持；

.3 實施和執行港口設施保安計劃；

.4 對港口設施進行定期保安檢查，確保適當保安措施的繼續；

.5 適視建議和列入港口設施保安計劃的修正案，以糾正缺陷，更新計劃並計及港口設施的有關改變；

.6 提高港口設施人員的保安意識和警惕；

.7 確保已向負責港口設施保安的人員提供了適當培訓；

.8 向有關當局報告發生的威脅港口設施保安的事件並保管此種事件的記錄；

.9 與適當的公司和船舶保安官員協調港口設施保安計劃的實施；

.10 視情與保安業務協調；

.11 確保達到負責港口設施保安的人員的標準；

.12 確保保安設備（如果有的話）的正確操作、測試、校準和保養；和

.13 在被要求時，幫助船舶保安官員確認要上船人員的身份。

17.3 應向港口設施保安官員提供履行其第 XI-2 章和本規則的本部分規定的職責和責任的必要幫助。

18 港口設施保安培訓、操練和演習

18.1 計及本規則第 B 部分中的指導，港口設施保安官員和適當的港口設施保安人員應具有知識並接受過培訓。

18.2 計及本規則第 B 部分中的指導，有具體保安職責的港口設施人員應了解港口設施保安計劃中陳述的其港口設施保安職責和責任並應有足夠的知識和能力履行被指定的職責。

18.3 計及本規則第 B 部分中的指導，為確保港口設施保安計劃的有效實施，應計及港口設施的運營類型、港口設施人員的變化、港口設施服務的船型和其他有關情況，每隔適當時間進行操練。

18.4 計及本規則第 B 部分中的指導，港口設施保安官員應每隔適當時間參加演習，確保港口設施保安計劃的有效協調和實施。

19 船舶核查和發證

19.1 核查

19.1.1 本規則的本部分適用的每一船舶應接受下述核查：

.1 初次核查。在船舶投入營運之前或在首次頒發第 19.2 節規定的證書前進行。它應包括對第 XI-2 章和本規則的本部分和經核准的船舶保安計劃的有關規定涉及的保安系統和任何相關的保安設備的完整核查。該核查應確保船舶的保安系統和任何相關的保安設備完全符合第 XI-2 章和本規則的本部分的適用要求，處於令人滿意的狀況並適合該船的預定營運；

.2 更證核查。在主管機關規定的但不超過五年的間隔期舉行，但 19.3 節適用者除外。該核查應確保船舶的保安系統和任何相關的保安設備完全符合第 XI-2 章、本規則的本部分和經核准的船舶保安計劃的適用要求，處於令人滿意的狀況並適合該船的預定營運；

.3 中期核查。至少進行一次。如果僅進行一次中期核查，則它應在第 I/2（n）條規定的證書的第二和第三個周年日之間進行。中期核查應包括對船舶的保安系統和任何相關的保安設備的檢查，確保船舶仍然適合其預定營運。此種中期核查應在證書上作出簽註；

.4 任何額外核查。由主管機關確定。

19.1.2 船舶核查應由主管機關的官員進行。但主管機關可將核查委託給第 XI-2/1 條中所述的經認可的保安組織。

19.1.3 在每一情況下，有關主管機關應充分保證核查的完整性和有效性並應承諾確保作出履行該義務的必要安排。

19.1.4 在核查後，船舶的保安系統和任何相關的保安設備應保持符合第 XI-2/4.2 和 XI-2/6 條、本規則的本部分和經核准的船舶保安計劃的規定。在 19.1.1 節規定的任何核查完成後，未經主管機關同意不得對保安系統和任相關的保安設備或經認可的船舶保安計劃作出任何更改。

19.2 證書的頒發和簽註

19.2.1 在按 19.1 節的規定完成了初次或更證核查後應頒發“國際船舶保安證書”。

19.2.2 此種證書應由主管機關或代表主管機關行事的經認可的保安組織頒發或簽註。

19.2.3 應主管機關請求，另一締約政府可對該船作出核查，如認為符合 19.1.1 節的規定，應向該船頒發或授權頒發“國際船舶保安證書”，並且，如適當，應按本規則對船舶的該證書作出或授權作出簽註。

19.2.3.1 應儘早向作出請求的主管機關發送證書的副本和核查報告的副本。

19.2.3.2 以此種方式頒發的證書應載有證書係應主管機關的請求頒發的聲明；它應與根據 19.2.2 節頒發的證書得到同樣的承認。

19.2.4 “國際船舶保安證書”應使用本規則附錄中所載樣本的相應格式製成。如果使用的語文不是英文、法文或西班牙文，則條文應包括其中一種語文的譯文。

19.3 證書的期限和有效性

19.3.1 “國際船舶保安證書”應在主管機關規定的、不超過五年的期限頒發。

19.3.2 當更證核查係在現有證書失效日期前的三個月內完成時，新證書應從更證核查的完成日期至從現有證書的失效日期起算不超過五年的某一日期有效。

19.3.2.1 當更證核查係在現有證書的失效日期後完成時，新證書應從更證核查的完成日期至從現有證書的失效日期起算不超過五年的某一日期有效。

19.3.2.2 當更證核查係在現有證書的失效日期前多於三個月完成時，新證書應從更證核查的完成日期至從更證核查的完成日期起算不超過五年的某一日期有效。

19.3.3 如果係按不足五年的期限頒發，則主管機關可將證書的效力展至 19.3.1 節規定的最大期限，但應視情進行 19.1.1 節所述的、適用於五年頒證期限的核查。

19.3.4 如果更證核查業已完成而新證書卻不能在現有證書的失效日期前頒發或放在船上，則主管機關或代表主管機關行事的經認可的保安組織可對現有證書作出簽註。此種證書應在從失效日期起算不超過五個月的新期限中有效。

19.3.5 如在證書失效時船舶不在其預定的核查港口內，則主管機關可對證書的有效期作出延展，但給予此種展期的目的僅限於使船舶能夠完成抵達其預定核查港的航行並僅在這樣做是正當和合理的情況下。證書的展期不應超過三個月，獲得展期的船舶在到達其預定核

查港口後無權根據此種展期在沒有新證書的情況下離開該港口。在完成更證核查後，新證書應在至從現有證書被展期前的失效的日期起算不超過五年的某一日期止的期限內有效。

19.3.6 向從事國際航行的船舶頒發的、未根據本節的上述規定予以展期的證書，可由主管機關在從證書載明的失效日期起算不超過一個月的寬期內予以展期。在更證核查完成後，新證書應在至從現有證書展期前的失效日期起算不超過五年的某一日期止的期限內有效。

19.3.7 如果中期核查在 19.1.1 節規定的期限前完成，則：

.1 應通過簽註將證書上所載的失效日期修改為從中期核查的完成日期起算不超過三年的某一日期；

.2 如進行了一次或多次額外核查從而不超過 19.1.1 節規定的最大核查間隔期，則失效日期可以不變。

19.3.8 根據 19.2 節頒發的證書在下列任一情況下應失效：

.1 在 19.1.1 節規定的期限內未完成有關核查；

.2 如適用，證書未按 19.1.1.3 和 19.3.7.1 節作出簽註；

.3 公司承擔對該公司先前未經營的船舶的營運責任；和

.4 在船舶換掛另一國家的國旗時。

19.3.9 如果：

.1 船舶換掛另一締約政府的國旗，則該船先前有權懸掛其國旗的締約政府應儘早將該船在換掛船旗前持有的“國際船舶保安證書”的副本或與該證書相關的所有信息和現有核查報告的副本發給接收的主管機關，或

.2 公司承擔該公司先前未經營的船舶的營運責任，則以前的公司應儘早將與“國際船舶保安證書”相關的所有信息的副本發給接收的公司，以便利 19.4.2 節中所述的核證。

19.4 臨時證書

19.4.1 19.2 節中規定的證書只有在頒發該證書的主管機關確和該船符合 19.1 節的要求時才能頒發。但在 2004 年 7 月 1 日後，就下述情況而言：

.1 船舶在交船時或在投入或重新投入營運前沒有證書；

.2 船舶將一締約政府的國旗換為另一締約政府的國旗；

.3 船舶將非締約政府的國旗換為締約政府的國旗；或

.4 公司承擔了該公司先前未經營的船舶的營運責任。

在頒發 19.2 節所述的證書前，主管機關可頒發“臨時國際船舶保安證書”，其格式應相應於本規則的本部分的附錄中的樣本。

19.4.2 “臨時國際船舶保安證書”只有在主管機關或代表主管機關行事的經認可的組織已證實以下情況後才能頒發：

.1 已完成本規則的本部分要求的船舶保安評定；

.2 在船上備有符合第 XI-2 章和本規則第 A 部分的要求的船舶保安計劃的副本，它已被提交供檢查和核准並在船上得到實施；

.3 如要求，船舶配有符合第 XI-2/6 條的要求的船舶保安警戒系統；

.4 公司保安官員：

.1 已確保：

.1 對船舶保安計劃作出檢查，以符合本規則的本部分；

.2 計劃已被提交供核准；和

.3 計劃正在船上得到實施；和

.2 已作出必要安排，包括操練、演習和內部審核安排，從而確信該船在六個月內會合格完成 19.1.1.1 節規定的核查；

.5 已作出安排進行 19.1.1.1 節中規定的核查；

.6 船長、船舶保安官員和具有具體保安職責的其他船舶人員熟知本規則的本部分中規定的其職責和責任和在船上放置的船舶保安計劃的有關規定，得到了以船舶人員的工作語文或其懂得的語文寫成的此種信息；和

.7 船舶保安官員符合本規則的本部分的要求。

19.4.3 “臨時國際船舶保安證書”可由主管機關或被授權代表其行事的經認可的保安組織頒發。

19.4.4 “臨時國際船舶保安證書”的有效期應為六個月，或至 19.2 節要求的證書被頒發，以早者為準，不得展期。

19.4.5 如主管機關或經認可的保安組織斷定船舶或公司要求此種證書的目的之一是要避免在 19.4.4 節規定的首個“臨時證書”的期限後完全符合第 XI-2 章和本規則的本部分，則任何締約政府均不應向該船頒發以後的相續“臨時國際船舶保安證書”。

19.4.6 就第 XI-2/9 條而言，締約政府可在將“臨時國際船舶保安證書”接受為有效證書前確保 19.4.2.4 至 19.4.2.6 節的要求已獲滿足。

第 A 部分的附錄

附錄 1

國際船舶保安證書的格式

國際船舶保安證書

（官方鋼印） *（國名）*

證書編號.....

本證書係經.....政府授權，由.....

（國名） *（經授權的人員或組織）*

根據《國際船舶和港口設施保安規則》(《ISPS 規則》) 的規定頒發

船名 ：.....

識別編號或字符 ：.....

登記港 ：.....

船型 ：.....

總噸位 ：.....

IMO 編號 ：.....

公司名稱和地址 ：.....

茲證明：

1 該船的保安系統和任何相關保安設備已按《ISPS 規則》第 A 部分 19.1 節作出核查；

2 核查表明該船的保安系統和任何相關保安設備在所有方面均令人滿意，該船符合本公約第 XI-2 章和《ISPS 規則》第 A 部分的適用要求；

3 該船備有經核准的船舶保安計劃。

作為本證書基礎的初次/更證核查日期：.....

本證書有效至.....

但須接受《ISPS 規則》第 A 部分 19.1.1 節規定的核查。

頒發地點.....

（證書頒發地）

頒發日期..... .....

（經正式授權的發證官員的簽字）

（發證當局的鋼印或章印）

中期核查的簽註

茲證明在《ISPS 規則》第 A 部分 19.1.1 節要求的中期核查中查明該船符合本公約第 XI-2 章和《ISPS 規則》第 A 部分的有關規定。

中期核查 簽字.....

（經授權官員的簽字）

地點.....

日期.....

（當局的鋼印或章印）

額外核查的簽註

額外核查 簽字.....

（經授權官員的簽字）

地點.....

日期.....

（當局的鋼印或章印）

額外核查 簽字.....

（經授權官員的簽字）

地點.....

日期.....

（當局的鋼印或章印）

額外核查

簽字.....

（經授權官員的簽字）

地點.....

日期.....

（當局的鋼印或章印）

《ISPS 規則》第 A/19.3.7.2 節規定的額外核查

茲證明在《ISPS 規則》第 A 部分 19.3.7.2 節要求的額外核查中查明該船符合本公約第 XI-2 章和《ISPS 規則》第 A 部分的有關規定。

簽字.....

（經授權官員的簽字）

地點.....

日期.....

（當局的鋼印或章印）

在《ISPS 規則》第 A/19.3.3 節適用時有效期不足五年的證書的展期簽註

該船符合《ISPS 規則》第 A 部分的有關規定，該證書應按《ISPS 規則》第 A 部分 19.3.3 節被接受為有效，直至.....

簽字.....

（經授權官員的簽字）

地點.....

日期.....

（當局的鋼印或章印）

在更證核查業已完成並且《ISPS 規則》

第 A/19.3.4 節適時的簽註

該船符合《ISPS 規則》第 A 部分的有關規定。該證書應按《ISPS 規則》第 A 部分 19.3.4 節被接受為有效，直至.....

簽字.....

（經授權官員的簽字）

地點.....

日期.....

（當局的鋼印或章印）

在《ISPS 規則》第 A/19.3.5 節適用時將證書展期至抵達核查港口或在《ISPS 規則》第 A/19.3.6 節適用時對證書作寬限展期的簽註

該證書應按《ISPS 規則》第 19.3.5/19.3.6*節被接受為有效，直至.....

簽字.....

（經授權官員的簽字）

地點.....

日期.....

（當局的鋼印或章印）

在《ISPS 規則》第 A/19.3.7.1 節適用時將失效日期推遲的簽註

按《ISPS 規則》第 A 部分 19.3.7.1 節，新的失效日期**是.....

簽字.....

（經授權官員的簽字）

地點.....

日期.....

（當局的鋼印或章印）

---

* 視情刪去。

** 在填寫證書的本部分時，證書封面上的失效日期也應作相應修改。

附錄 2

“臨時國際船舶保安證書”的格式

臨時國際船舶保安證書

（官方鋼印） *（國名）*

證書編號.....

本證書係經.....政府授權，由.....

（國名） *（經授權的人員或組織）*

根據《國際船舶和港口設施保安規則》(《ISPS 規則》) 的規定頒發

船名 ：.....

識別編號或字符 ：.....

登記港 ：.....

船型 ：.....

總噸位 ：.....

IMO 編號 ：.....

公司名稱和地址 ：.....

是否是以後的相繼“臨時證書”？是/不是*

如果是，則首個“臨時證書”的頒發日期為.....

---

* 視情刪去。

茲證明符合《ISPS 規則》第 A/19.4.2 節的要求。

本證書係按《ISPS 規則》第 A/19.4 節頒發。

本證書有效期至.....

頒發地點.....

（證書頒發地）

頒發日期..... .....

（經正式授權的發證官員的簽字）

（發證當局的鋼印或章印）

第 B 部分

關於經修正的《1974 年國際海上人命安全公約》附件

第 XI-2 章和本規則第 A 部分的規定的指導

1 前言

綜述

1.1 本規則的序言指出：第 XI-2 章和本規則第 A 部分確立了強化海上保安的保安措施及船舶和港口設施合作偵查和阻止威脅海上運輸保安行為的國際框架。

1.2 本前言簡述了在制定和實施達到並保持符合第 XI-2 章和本規則第 A 部分的規定所需的措施和安排，指明了要提供指導的主要內容。該指導載於 2 至 19 段中。它還確定了在考慮將本指導應用於船舶和港口設施時應計及的必要考慮事項。

1.3 如果讀者的興趣僅限於船舶，則強烈建議仍將本規則的本部分視為一個整體，特別是有關港口設施的段落。對其主要興趣是港口設施的人而言，這也同樣適用；他們也應閱讀有關船舶的段落。

1.4 在以下段落中提供的指導係主要關於對在港口設施中的船舶的保護。但可能出現船舶會對港口設施構成威脅的情況，如出於在港口中時它可被用作進行襲擊的基地。在考慮因應船上保安威脅的適當保安措施時，填寫港口設施保安評定或準備港口設施保安計劃的人員應考慮對在下列段落中提供的指導作出適當調整。

1.5 要敬告讀者的是：不應將本規則的本部分中的任何規定理解或解釋成與第 XI-2 章或本規則第 A 部分的任何規定有任何衝突。上述規定應始終壓倒和否定在本規則的本部分中可能因疏忽而出現的非有意的不一致性。本規則的本部分中的指導始終應以與第 XI-2 章和本規則第 A 部分確立的目的、目標和原則相符的方式來理解、解釋和應用。

締約政府的責任

1.6 根據第 XI-2 章和本規則第 A 部分的規定，締約政府有各種責任，其中包括：

— 確定適用的保安級別；

— 核准船舶保安計劃（SSP）和先前核准的計劃的修正案；

— 核查船舶是否符合第 XI-2 章和本規則第 A 部分的規定和向船舶頒發“國際船舶保安證書”；

— 確定需對在其領土內的哪些港口設施任命負責準備港口設施保安計劃的港口設施保安官員（PFSO）；

— 確保港口設施保安評定（PFSA）的完成和核准；

— 核准港口設施保安計劃（PFSP）和先前核准的計劃的任何此後修正案；

— 執行控制和符合措施；

— 檢驗經核准的計劃；和

— 向國際海事組織和航運和港口業傳答信息。

1.7 締約政府可在其政府內指定或設立“指定當局”以履行第 XI-2 章和本規則第 A 部分中規定的其對港口設施的保安責任和准許經認可的保安組織進行有關港口設施的若干工作，但對接受和核准該工作的最後決定應由締約政府或“指定當局”作出。主管機關也可以將履行有關船舶的若干保安職責的工作委託給經認可的保安組織。但下列職責或活動不能委託給經認可的保安組織：

— 確定適用的保安級別；

— 確定需對在締約政府領土內的哪些港口設施任命 PFSO 或準備 PFSP；

— 核准 PFSA 或先前核准的評定的任何此後修正案；

— 核准 PFSP 或先前核准的計劃的任何此後修正案；

— 執行控制和符合措施；和

— 確定對“保安聲明”的要求。

確定保安級別

1.8 確定在任何特定時間使用的保安級別是締約政府責任，能適用於船舶和港口設施。本規則第 A 部分對供國際使用的三個保安級別作出了定義。它們是：

— 正常情況下的 1 級保安：船舶和港口設施正常運行的保安級別；

— 更大風險時的 2 級保安：在有更大的保安事件風險時使用的級別；

— 異常情況下的 3 級保安：在有可能或立即的保安事件風險時使用的級別。

公司和船舶

1.9 經營適用於第 XI-2 章和本規則第 A 部分的船舶的公司必須為公司任命一位 CSO 和為其每一船舶任命一位 SSO。這些官員的職責、責任和培訓要求以及操練和演習要求在本規則的第 A 部分作了規定。

1.10 公司保安官員的責任包括：簡而言之，確保船舶保安評定（SSA）正確開展，確保 SSP 被制定並提交供主管機關或其代表核准並在此後置於本規則第 A 部分適用的、該人員被任命為其 CSO 的每一船舶上。

1.11 SSP 應指明該船自己應採取的確保它始終在 1 級保安下運行的操作和有形保安措施。該計劃還應指明該船自己應採取的在接到指示時升級到 2 級保安並在該級別下運行的額外或強化的保安措施。此外該計劃應指明該船能夠採取的可能準備行動，以便對保安事件或其威脅的反應的人員在 3 級保安時可能發出的指示作出迅速反應。

1.12 適用於第 XI-2 章和本規則第 A 部分的要求的船舶需要有經主管機關或其代表核准的 SSP 並按該計劃運行。CSO 和 SSO 應監視該計劃的繼續相關性和有效性，包括進行內部審核。經核准的計劃的任何成分的修正案，如係主管機關確定的需經核准者，則須在提交供檢查和核准後才能列入經核准的計劃並由船舶實施。

1.13 船舶必須攜帶註明它符合第 XI-2 章和本規則第 A 部分的要求的“國際船舶保安證書”。本規則第 A 部分包括有關在初次、更證和中期核查的基礎上核查和驗證船舶符合要求的規定。

1.14 當船舶在某一締約政府的港口內或正在駛往此種港口時，該締約政府根據第 XI-2/9 條的規定有權對該船執行各種控制和符合措施。該船應接受港口國控制檢查，但除特定情況外，檢查通常不應延伸至對 SSP 本身的檢查。如執行控制和符合措施的締約政府有理由相信船舶的保安或其服務的港口設施的保安受到損害，則可對船舶執行額外的控制措施。

1.15 船舶還需在船上備有指明誰是負責決定船上人員的僱用和決定與船舶使用有關的各種問題的人員的信息，以便在有此要求時提供給締約政府。

港口設施

1.16 每一締約政府必須確保完成在其領土內的、服務於從事國際航行的船舶的每一港口設施的 PFSA。締約政府、“指定當局”或經認可的保安組織可進行該評定。完成的 PFSA 須由締約政府或有關的指定當局核准。該核准不准委託他人。應定期對港口設施保安評定作出檢查。

1.17 從根本上說，PFSA 是對港口設施運作的所有方面的風險分析，以確定其中哪些部分更容易和/或更可能成為襲擊對象。保安風險是襲擊風險與目標弱點和襲擊後果的一種函數關係。

評定必須包括以下成分：

— 確定對港口裝置和基礎設施的已知威脅；

— 識別潛在弱點；和

— 計算事件後果。

在完成分析後便可能產生對風險程度的全面評定。PFSA 有助於確定哪些港口設施須任命 PFSO 和需準備 PFSP。

1.18 必須符合第 XI-2 章和本規則第 A 部分的要求的港口設施需任命 PFSO。這些官員的職責、責任和培訓要求和對操作和演習的要求在本規則第 A 部分中作了規定。

1.19 PFSP 應指明港口設施應採取的確保它始終在 1 級保安下運行的操作和有形保安措施。該計劃還應指明港口設施能夠採取的在接到指示時升級到 2 級保安並在該級別下運行的額外或強化的保安措施。此外，該計劃應指明港口設施能夠採取的準備行動，以便對保安事件或其威脅的反應人員在 3 級保安下可能發出的指示作出迅速反應。

1.20 必須符合第 XI-2 章和本規則第 A 部分的要求的港口設施需備有經締約政府或有關“指定當局”核准的 PFSP 並按該計劃運作。PFSO 應實施其規定並監視該計劃的繼續有效性和相關性，包括對計劃的應用作出內部審核。經核准的計劃的任何成分的修正案，如係主管機關或有關“指定當局”確定的需要核准者，則必須在提交供檢查和核准後才能列入經核准的計劃中和在港口設施中予以實施。締約政府和有關的“指定當局”可檢驗計劃的有效性。應定期對有關港口設施的或作為制定計劃的基礎的 PFSA 作出檢查。所有這些活動均可能導致對經核准的計劃作出修正。經核准的計劃的規定內容的任何修正案均必須提交供締約政府或有關“指定當局”核准。

1.21 可對使用港口設施的船舶執行第 XI-2/9 條中所述的港口國控制檢查和額外控制措施。在船舶進入港口前，有關當局可要求提供有關船舶及其貨物、旅客和船舶人員的信息。在有些情況下可拒絕船舶入港。

信息和通信

1.22 第 XI-2 章和本規則第 A 部分要求締約政府向國際海事組織提供若干信息並要求使信息可以獲得，以保障締約政府間、公司保安官員/船舶保安官員和港口設施保安官員間的有效通信。

2 定義

2.1 未對第 XI-2 章和本規則第 A 部分中的定義提供任何指導。

2.2 就規則的本部分而言：

.1 “節”係指本規則第 A 部分的某一節，表示為“第 A/（後接節編號）節”；

.2 “段”係指本規則的本部分的某一段，表示為“第（段編號）段”；和

.3 “締約政府”在第 14 至 18 段中使用時係指“港口設施在其領土內的締約政府”並包括對“指定當局”的提及。

3 適用範圍

綜述

3.1 在實施第 XI-2 章和本規則第 A 部分的要求時應計及本規則的本部分中的指導。

3.2 但應認識到船舶指導的適用範圍取決於船型、其貨物和/或旅客、其運輸方式和船舶到訪的港口設施的特點。

3.3 同樣，就港口設施指導而言，指導的適用範圍取決於港口設施、使用港口設施的船舶類型、貨物和旅客的類型和到訪船舶的運輸方式。

3.4 第 XI-2 章和本規則第 A 部分的規定不適用於主要為軍事目的設計和使用的港口設施。

4 締約政府的責任

評定和計劃的保安

4.1 締約政府應確保有就位的適當措施來避免擅自洩露或查閱與船舶保安評定（SSA）、船舶保安計劃（SSP）、港口設施保安評定（PFSA）和港口設施保安計劃（PFSP）有關的保安敏感資料和各個評定或計劃。

指定當局

4.2 締約政府可確定由政府內的某一“指定當局”履行第 XI-2 章和本規則第 A 部分規定的其港口設施保安職責。

經認可的保安組織

4.3 締約政府可授權經認可的保安組織（RSO）開展若干保安活動，包括：

.1 代表主管機關核准船舶保安計劃或其修正案；

.2 代表主管機關核查和驗證船舶對第 XI-2 章和本規則第 A 部分的要求的符合；

.3 進行締約政府要求的港口設施保安評定。

4.4 RSO 可就保安事項向公司或港口設施提供建議或幫助，包括船舶保安評定、船舶保安計劃、港口設施保安評定和港口設施保安計劃。這可包括完成 SSA、SSP、PFSA 或 PFSP。如果 RSO 對 SSA 或 SSP 提供了建議或幫助，就不應授權該 RSO 來核准該 SSP。

4.5 在向 RSO 作出授權時，締約政府應考慮此種組織是否勝任。RSO 應能證實：

.1 在有關保安事項上的專長；

.2 對船舶和港口作業的適當知識，如為船舶提供服務，則包括對船舶設計和構造的知識；如為港口設施提供服務，則包括對港口設計和構造的知識；

.3 對在船舶和港口作業期間發生的可能保安風險作出評定的能力，包括船/港界面和如何使此種風險最小化；

.4 保持和提高其人員的專長的能力；

.5 監視其人員是否繼續值得信任的能力；

.6 保持適當措施避免擅自洩露和查閱保安敏感資料的能力；

.7 對第 XI-2 章和本規則第 A 部分的要求和對有關的國家和國際立法和保安要求的知識；

.8 對當前的保安威脅及其方式的知識；

.9 對識別和探測武器、危險物質和裝置的知識；

.10 對在無歧視的基礎上識別可能威脅保安的人員的特點和行為方式的知識；

.11 對逃避保安措施使用的技術的知識；和

.12 對保安和監視設備和系統及其操作局限性的知識。

在向 RSO 委託具體職責時，包括主管機關在內的締約政府應確保該 RSO 具備執行該任務所需的勝任能力。

4.6 第 I/6 條中所述的、符合第 XI-1/1 條要求的經認可的組織，如具備 4.5 款中所列的適當保安專門知識，則可被指定為 RSO。

4.7 港口當局或港口設施的經營人，如具備 4.5 款中所列的適當保安專長，則可被指定為 RSO。

確定保安級別

4.8 在設定保安級別時，締約政府應計及一般和具體的威脅信息。締約政府應對船舶和港口設施確定以下三個級別中的某一保安級別：

— 正常狀況下的 1 級保安：船舶或港口設施正常運行的保安級別；

— 更大風險時的 2 級保安：在有更大保安事件風險時使用的級別；和

— 異常情況下的 3 級保安：在有保安事件的可能或立即風險時使用的級別。

4.9 設定 3 級保安是一種異常的措施，僅在有可靠信息表明有可能或立即的保安事件時才使用。3 級保安僅在有確定的保安威脅或實際的保安事件期間設定。雖然保安級別可依次從 1 級保安變為 2 級保安再變為 3 級保安，但從 1 級保安直接變為 3 級保安也是可能的。

4.10 船長始終對船舶的安全和保安負有最高責任。如有理由相信遵守對保安事件或其威脅的反應的人員發出任何指示可能損害船舶的安全，則即使在 3 級保安時，船長也可要求對此種指示作出澄清或修正。

4.11 CSO 或 SSO 應儘早與船舶要到訪的港口設施的 PFSO 取得聯繫以查明在港口設施中對該船使用的保安級別。PFSO 在與船舶建立聯繫後應將港口設施保安級別的此後的任何變化通知船舶並向船舶提供任何有關的保安信息。

4.12 雖然可以有某一船舶的保安級別要高於其要到訪的港口設施的情況，但在任何情況下船舶的保安級別不可低於其要到訪的港口設施。如果船舶的保安級別高於其要使用的港口設施，則 CSO 或 SSO 應向 PFSO 作出及時通知。PFSO 應與 CSO 或 SSO 進行磋商，對特定的情況作出評定，與船舶議定適當的保安措施，包括填寫和簽署“保安聲明”。

4.13 締約政府應考慮如何迅速發佈保安級別更改信息。主管機關可將 NAVTEX 報文或“航海通告”作為向船舶及 CSO 和 SSO 通知保安級別的此種更改的方法。或者，他們也可考慮提供同等或更好的速度和覆蓋範圍的其他通信方法。締約政府應確定向 PFSO 通知保安級別更改的方法。締約政府應編輯和保持需向其通報保安級別更改的人員的聯絡細節。雖然不必將保安級別視為是特別敏感的，但涉及的威脅信息卻可能是高度敏感的。締約政府應對傳達的信息的類型和詳情以及向 SSO、CSO 和 PFSO 傳達此種信息的方法作出認真考慮。

聯絡點和港口設施保安計劃信息

4.14 在港口設施有 PFSP 時，應將該情況通知本組織並且必須將信息提供給 CSO 和 SSO。除有就位的 PFSP 外，不必公佈其任何進一步細節。締約政府應考慮設立中央或區域聯絡點或提供有關有就位的 PFSP 的地點以及有關的 PFSO 的聯絡細節的最新信息的其他方法。對有此種聯絡點一事應予以公佈。他們也可提供有關被指定代表該締約政府行事的經認可的保安組織以及此種經認可的保安組織的具體責任和授權條件的信息。

4.15 對於沒有 PFSP（因而也沒有 PFSO）的港口，中央或區域聯絡點應能確定一位在必要時能在船舶到訪期間作出使適當保安措施就位的安排的有適當資格的岸上人員。

4.16 締約政府還應提供 SSO、CSO 和 PFSO 能向其報告保安關切事項的政府官員的聯絡詳情。這些政府官員應在採取適當行動前評定此種報告。此種報告的關切事項可能對另一締約政府管轄範圍內的保安措施有影響。在此種情況下，締約政府應考慮與該另一締約政府的相應官員聯絡，以討論補救措施是否適當。為此，應向國際海事組織通報這些政府官員的聯絡細節。

4.17 在有此要求時，締約政府應向其他締約政府提供 4.14 至 4.16 段中指明的信息。

身份證

4.18 鼓勵締約政府向在履行其官方職責時有權上船或進入港口設施的政府官員頒發適當的身份證並制定核查此種文件的真實性的程序。

固定和浮動平台和就位的移動式近海鑽井裝置

4.19 締約政府應考慮制定固定和浮動平台和就位的移動式近海鑽井裝置的適當保安措施，以符合第 XI-2 章和本規則第 A 部分的規定所需的與船舶的互動。

不需符合本規則第 A 部分的船舶

4.20 締約政府應考慮制定適當保安措施來強化第 XI-2 章和本規則第 A 部分不適用的船舶的保安，確保適用於此種船舶的任何保安規定均允許與本規則第 A 部分適用的船舶的互動。

對船舶的威脅和其他海上事件

4.21 締約政府應考慮對被視為適於減少對懸掛其國旗的船舶在海上時的保安風險的措施提供指導。它們應對在下列情況下按 1 至 3 級保安要採取的行動提供具體意見：

.1 船舶在海上時適用於該船的保安級別有變化，如由於其運營的地理區域或與該船本身有關的地理區域的原因；和

.2 在海上時有涉及該船的保安事件或其威脅。

締約政府應制定用於此種目的的最好方法和程序。在即將發生襲擊的情況下，船舶應努力與船旗國負責保安事件反應的人員建立直接通信。

4.22 締約政府還應設立向下列者提供保安建議的聯絡點：

.1 有權懸掛其國旗的任何船舶；或

.2 在其領海中運行的或已通報欲進入其領海意圖的任何船舶。

4.23 締約政府應向在其領海中運行的或已通報欲進入其領海意圖的船舶提出建議，包括下列建議：

.1 改變或推遲意圖的通過；

.2 在特定航線航行或駛往特定地點；

.3 能否提供可放置到船舶上的任何人員或設備；

.4 對通過、抵港或離港作出協調，以便由巡邏艇或飛機（固定機翼或直升飛機）護航。

締約政府應提醒在其領海中運行的或已通報欲進入其領海意圖的船舶注意其公佈的任何臨時禁區。

4.24 締約政府應建議在其領海中運行的或已通報欲進入其領海意圖的船舶立即實施該締約政府建議的任何保安措施，以保護該船或附近的其他船舶。

4.25 締約政府為 4.22 段所述目的準備的計劃應包括有關在包括主管機關在內的該締約政府中的、每天 24 小時均可使用的適當聯絡點的信息。這些計劃還應包括有關於主管機關認為在何種情況下應尋求附近沿海國的幫助的信息和 PFSO 和 SSO 間的聯絡程序。

替代保安協議

4.26 締約政府在考慮如何實施第 XI-2 章和本規則第 A 部分時，可與一個或多個締約政府締結一個或多個協議。協議的範圍限於在該協議當事方領土內港口設施間固定航線上的短途國際航行。在締結協議之時或之後，這些締約政府應與對該協議的影響有利害關係的其他

締約政府和主管機關協商。懸掛非該協議當事方的國旗的船舶，只有在其主管機關同意該船應遵守協議的規定並要求該船這樣做時，才應被允許在協議中規定的固定航線上運行。在任何情況下此種協議均不得損害未被其涉及的其他船舶和港口設施的保安水平，特別是此種協議涉及的所有船均不得與未涉及的船舶進行船對船的活動。協議涉及的船舶採用的任何操作界面均應由其作出規定。必須連續監視每一協議的運作，在必要時對其作出修正，在任何情況下均應每五年對其作出一次檢查。

港口設施的等效安排

4.27 對於有有限或特別作業的但並非偶爾才有交通的若干特定港口設施，使用等效於第 XI-2 章和本規則第 A 部分規定者的保安措施來確保符合可能是適當的。對於工廠的附屬碼頭或不常有作業的岸壁碼頭則尤其如此。

配員水平

4.28 在確定船舶的最低安全配員水平時，主管機關應計及第 V/14 條規定的最低安全配員水平僅涉及船舶的安全航行。主管機關還應計及實施 SSP 可能引起的額外工作量，確保船舶的足夠和有效配員。主管機關在這樣做時應根據對各船上人員指定的所有船上職責核實船舶能執行國家法律公佈的休息小時和防止疲勞的其他措施。

控制和符合措施

綜述

4.29 第 XI-2/9 條陳述了第 XI-2 章中適用於船舶的控制和符合措施。它分為三個明確的部分：對港內船舶的控制、對要進入另一締約政府的港口的船舶的控制和適用於這兩種情況的額外規定。

4.30 第 XI-2/9.1 條“對港內船舶的控制”實施了當船舶在締約政府的正式授權官員（“正式授權官員”）有權上船核查規定的證書均符合要求的外國港口中時的一種船舶控制制度。如有明確理由認為該船不符合規定，則可採取控制措施，如額外檢查或扣船。這反映了現行的控制制度。第 XI-2/9.1 條是以此種制度為基礎的，計及了在正式授權官員有明確理由認為船舶不符合第 XI-2 章或本規則第 A 部分的規定時的額外措施（包括將船舶驅逐出港作為一種控制措施）。第 XI-2/9.3 條陳述了促進公正和適度實施這些額外措施的保護措施。

4.31 第 XI-2/9.2 條向欲進入另一締約政府的港口的船舶應用確保符合的控制措施並採用了第 XI-2 章內僅適用於保安的完全不同概念。根據該條，為更好地確保保安，可在船舶的進港前實施措施。如同在第 XI-2/9.1 條中一樣，該額外控制制度是以有明確理由相信船舶不符合第 XI-2 章或本規則第 A 部分的概念為基礎的，並包括了第 XI-2/9.2.2、XI-2/9.2.5 和 XI-2/9.3 條中的重要保護措施。

4.32 船舶不符合要求的明確理由係指船舶不符合第 XI-2 章和本規則第 A 部分的要求的證據或可靠信息並計及本規則的本部分的指導。此種證據或可靠信息可來自正式授權官員在核查按規則第 A 部分頒發的船舶的“國際船舶保安證書”或“臨時國際船舶保安證書”（“證書”）時得出的專業判斷或看法或來自其他來源。即使船上有有效證書，正式授權官員仍可根據專業判斷有明確理由相信該船不符合要求。

4.33 XI-2/9.1 和 XI-2/9.2 條規定的可能明確理由的例子在相關時可包括：

.1 檢查無效或過期證書得到的證據；

.2 有關第 XI-2 章和本規則第 A 部分規定的保安設備、證件或安排有嚴重缺陷的證據或可靠信息；

.3 收到了報告或報怨，根據正式授權官員的專業判斷，其中有可靠信息清楚表明該船不符合第 XI-2 章和本規則第 A 部分的要求；

.4 正式授權官員使用專業判斷得到以下證據或看法：船長或船舶人員不熟習必要的船上保安程序或不能進行與船舶保安相關的操練，或未進行此種程序或操練；

.5 正式授權官員使用專業判斷得到以下證據或看法：船舶人員的主要成員不能與船舶人員中負有船上保安職責的任何其他主要成員建立正確溝通；

.6 下列證據或可靠信息：該船載有港口設施或另一船舶在違犯第 XI-2 章和本規則第 A 部分的情況下送到船上的人員、物料或貨物，而該船未填寫“保安聲明”，也未採取適當、特別或額外保安措施或未保持適當的船舶保安程序；

.7 下列證據或可靠信息：該船載有從無需符合第 XI-2 章或本規則第 A 部分的港口設施或另一來源（如另一船舶或直升飛機輸送）送到該船上的人員、物料或貨物，而該船未採取適當、特別或額外保安措施或未保持適當的保安程序；和

.8 船舶持有第 A/19.4 節規定的以後連續頒發的“臨時國際船舶保安證書”，而根據正式授權官員的專業判斷，

該船或公司要求此種證書的目的之一是為了避免在第A/19.4.4節規定的首個“臨時國際船舶安全證書”的期限後完全符合第XI-2章或本規則第A部分。

4.34 第XI-2/9條的國際法含意是特別有關的。在實施該條時應考慮到第XI-2/2.4條，因為可能出現要採取第XI-2章範圍外的措施或應考慮在第XI-2章中未予規定的受害船舶的權利的情況。因此第XI-2/9條不禁止締約政府，在船舶雖符合第XI-2章和本規則第A部分但仍被視為具有保安風險時，採取根據並符合國際法的措施確保人員、船舶、港口設施或其他財產的安全和保安。

4.35 在締約政府對船舶實施控制措施時，應及時與主管機關聯繫，提供足夠信息，使主管機關能與締約政府進行充分聯絡。

對港內船舶的控制

4.36 在導致扣船的不符是設備故障或有問題的證件並且在港口檢查時無法彌補此種不符時，締約政府可允許該船在符合港口國和主管機關議定的條件時駛往另一港口。

欲進入另一締約政府的港口的船舶

4.37 第XI-2/9.2.1條列出了締約政府作為進港條件要求船舶提供的信息。所列信息之一是確認船舶在某一港口設施的前十次掛靠期間採取的任何特別或額外措施。例子可包括：

.1 在掛靠非締約政府國家領土內港口期間採取的措施的記錄，特別是通常由締約政府領土內港口設施提供的措施；和

.2 與港口設施或其他船舶達成的任何“保安聲明”。

4.38 可作為進港條件要求列出的另一信息是確認在某一港口設施的前 10 次掛靠期間進行的船對船活動時保持了適當的船舶保安程序。通常不要求包括船舶在港口設施內傳輸引水員或海關、移民或保安官員或加燃料、過駁、裝供應品卸廢物的記錄，應為這些活動通常在 PFSP 的管轄範圍內。可提供的信息例子包括：

.1 與懸掛非締約政府的國家旗幟的船舶進行船對船活動時採取的措施的記錄，特別是通常由懸掛締約政府國旗的船舶提供的措施；

.2 與懸掛締約政府國旗但無需符合第 XI-2 章和本規則第 A 部分的規定的船舶進行船對船活動時採取的措施的記錄，如根據其他規定向該船頒發的任何保安證書的副本；和

.3 當船上有海上被營救的人員或貨物時，有關此種人員或貨物的所有已知信息，包括其已知身份和為查明被營救者的保安狀況代表船舶進行的任何核查的結果。第 XI-2 章或本規則第 A 部分沒有要延誤或禁止將海上遇險者送到安全地點的意圖。第 XI-2 章和本規則第 A 部分的唯一意圖是要向各國提供足夠的適當信息以保持其保安完整性。

4.39 可作為進港條件要求的、旨在幫助確保人員、港口設施、船舶和其他財產的安全和保安的其他實用保安信息的例子包括：

.1 “連續摘要記錄”中的信息；

.2 作出報告時的船位；

.3 船舶到港口的預定抵達時間；

.4 船員名單；

.5 對船上貨物的一般陳述；

.6 旅客名單；和

.7 第 XI-2/5 條要求攜帶的信息。

4.40 第 XI-2/9.2.5 條允許船長在得悉沿海或港口國將實施第 XI-2/9.2 條的控制措施後打消進港意圖。如船長打消該意圖，則第 XI-2/9 條便不再適用，但採取的任何其他步驟必須基於並符合國際法。

額外規定

4.41 在船舶被拒絕進港口或被驅逐出港的所有情況下，應將所有的已知情況通報有關國家的當局。如果知道的話，該通報應由下列者構成：

.1 船名，船旗、船舶識別號、呼號、船型和貨物；

.2 拒絕入港或驅逐出港口或港區的理由；

.3 如有關，任何保安不符情況的性質；

.4 如有關，為識別任何不符情況作出的任何努力的細節，包括對該船規定的任何航行條件；

.5 以前的掛靠港和下一聲明掛靠港；

.6 駛離時間和到達那些港口的可能預計時間；

.7 給船舶的任何指示，如作出航線報告；

.8 有關該船現行保安級別的現有信息；

.9 有關港口國與主管機關之間進行的任何通信的信息；

.10 為獲得進一步信息而作出報告的港口國國內聯絡點；

.11 船員名單；和

.12 任何其他有關信息。

4.42 要聯絡的有關國家應包括在船舶到下一港口的預定航線上國家，特別是在船舶打算進入該沿海國的領海時。其他有關國家可包括以前的掛靠港，以便取得進一步的信息和解決與以前的港口相關的保安問題。

4.43 在執行控制和符合措施時，正式授權官員應確保採取的任何措施或步驟是適度的。此種措施或步驟應是合理的，是糾正或減少不符情況所必需的最低嚴厲程度或最短時間。

4.44 第 XI-2/9.3.5.1 條中的“延誤”一詞也指由於根據本條採取的行動，船舶被不正當地拒絕入港或驅逐出港。

非當事國船舶或小於公約尺寸的船舶

4.45 對於懸掛非本公約締約政府的國旗或非《1988 年 SOLAS 議定書》[1]當事國的國旗的船舶，締約政府不應給與此種船舶更優惠的對待。因此應對此種船舶應用第 XI-2/9 條的要求和本規則的本部分中所載的指導。

4.46 應對小於公約尺寸的船舶實施維持保安的措施。採取此種措施時應充分考慮到第 XI-2 章的要求和本規則的本部分中的指導。

---

[1] 《1974 年國際海上人命安全公約的 1988 年議定書》。

5 保安聲明

綜述

5.1 “保安聲明”（DoS）應在港口設施的締約政府認為必要時或在船舶認為必要時填寫。

5.1.1 “DoS”的必要性可由港口設施保安評定（PFSA）的結果指明。在港口設施保安計劃（PFSP）中應對要求 DoS 的理由和情況作出陳述。

5.1.2 DoS 的必要性可由主管機關為有權懸掛其國旗的船舶指明或由船舶保安評定（SSA）的結果指明並應在船舶保安計劃（SSP）中寫明。

5.2 當船舶的保安級別高於港口設施或與其界面的另一船舶時，對於因該船（包括其貨物、旅客）或港口設施的情況或這些因素的組合的特定原因而對人員、財產或環境有較高風險的船/港界面或船對船活動，在較高保安級別可能要求 DoS。

5.2.1 當船舶或代表有權懸掛其國旗的船舶的主管機關要求填寫 DoS 時，港口設施保安官員（PFSO）或船舶保安官員（SSO）應對要求作出收迄通知並討論適當的保安措施。

5.3 在進行在經核准的 PFSA 中將其確定為特別關切的船/港界面活動前，PFSO 也可倡議 DoS。例子可包括旅客上、下船和危險或有害物質的過駁或裝卸。PFSA 也可指明需要 DoS 的在人口密集地區之中或附近的設施或在經濟上具有重要意義的作業。

5.4 DoS 的主要目的是確保船舶與港口設施或與其界面的其他船舶就各方將按各自的經核准的保安計劃的規定採取的各自的保安措施一事達成協議。

5.4.1 議定的 DoS 應視情由港口設施和船舶簽署和註明日期，指明符合第 XI-2 章和本規則第 A 部，並應包括其期限、有關保安級別和有關聯絡細節。

5.4.2 保安級別改變時可能需要填寫新的或經修訂的 DoS。

5.5 DoS 應視情使用英語、法語、西班牙語或港口設施和船舶的通用語文填寫。

5.6 DoS 的範本載於本規則的本部分的附錄 1 中。該範本是船舶和港口設施間的 DoS。如果是兩船間的 DoS，則應對範本作出適當調整。

6 公司的義務

綜述

6.1 第 XI-2/5 條要求公司向船長提供信息，以達到本條規定的公司要求。該信息應包括如下事項：

.1 負責任命船上人員的各方，如船舶管理公司、配員代理、承包商、特許經營人（如零售、批發和娛樂場等）；

.2 負責決定船舶使用的各方，包括定期或光船租賃人或以此種身份行動的其他實體；和

.3 在船舶係根據租船合同的條款被使用時：包括定期或船次租賃人在內的各方的聯絡細節。

6.2 按照第 XI-2/5 條，公司應在發生變化時應對信息作出更新和現行化。

6.3 該信息應使用英語、法語或西班牙語。

6.4 對於在 2004 年 7 月 1 日前建造的船舶，該信息應反映在該日期的實際狀況。

6.5 對於在 2004 年 7 月 1 日或以後建造的船舶和在 2004 年 7 月 1 日前建造的並在該日期已退役的船舶，該信息應從船舶投入營運之日起提供並反映在該日期的實際狀況。

6.6 如在 2004 年 7 月 1 日時船舶處於退役狀況，則在此日期後，該信息應從船舶重新投入營運之日起提供並反映在該日期的實際狀況。

6.7 前先提供的未反映在該日期的實際狀況的信息無需保留在船上。

6.8 在由另一公司承擔該船的經營責任時，在船上無需保存與先前經營該船的公司有關的信息。

此外，在 8、9 和 13 節中載有其他有關指導。

7 船舶保安

在第 8、9 和 13 節中載有有關指導。

8 船舶保安評定

保安評定

8.1 公司保安官員（CSO）負責確保對該公司船隊內需要符合第 XI-2 章和本規則第 A 部分的規定並由其負責的每一船舶進行船舶保

安評定（SSA）。雖然 CSO 不一定要親自履行與該職務相關的每一職責，但確保其得到正確履行的最後責任仍由各 CSO 承擔。

8.2 在開始 SSA 前，CSO 應確保利用了有關對船舶的預定掛靠港或旅客上下船港的威脅評定和有關這些港口設施及其保護措施的現有信息。CSO 應研究有關類似保安需要的前先報告。可行時，CSO 應會見船上和港口設施中的適當人員，討論評定的目的和方法。CSO 應遵守締約政府提供的任何具體指導。

8.3 SSA 應處理船上或船內的下列因素：

.1 有形保安；

.2 結構完整性；

.3 人員保護系統；

.4 程序政策；

.5 無線電和電信系統，包括電腦系統和網絡；和

.6 在受到破壞或用於非法觀察時會對船上或港口設施內的人員、財產或作業造成風險的其他方面。

8.4 參與執行 SSA 的人員應能在以下方面獲得專家幫助：

.1 對當前保安威脅和方式的知識；

.2 識別和探測武器、危險物質和裝置；

.3 在無歧視的基礎上對可能威脅保安的人員的特點和行為方式的識別；

.4 逃避保安措施使用的技術；

.5 造成保安事件使用的方法；

.6 爆炸品對船舶結構和設備的影響；

.7 船舶保安；

.8 船/港界面業務做法；

.9 應急規劃、應急防備和反應；

.10 有形保安；

.11 無線電和電信系統，包括電腦系統和網絡；

.12 輪機工程；

.13 船舶和港作業。

8.5 CSO 應取得並記錄進行評定所需的信息，包括：

.1 船舶的總佈局；

.2 駕駛台、A 類機器處所和第 II-2 章規定的其他控制站等限制進入區域的位置；

.3 每一實際或潛在的船舶通入點的位置和功能；

.4 對船舶保安弱點可能有影響的潮變化；

.5 貨物處所和積載裝置；

.6 船舶物料和重要維修設備的存放位置；

.7 寄存行李的存放位置；

.8 保持船舶重要業務的現有應急和備用設備；

.9 船舶人員的人數、任何現有的保安職責和任何現有的公司培訓要求做法；

.10 用以保護旅客和船舶人員的現有保安和安全設備；

.11 為確保有秩序和安全的船舶緊急撤離而需保持的脫險和撤離通道及集合站；

.12 與提供船/水側保安業務的私營保安公司達成的現有協議；和

.13 現行的現有保安措施和程序，包括檢查和控制程序、識別系統、監視和監測設備、人員身份證和通信、警報、照明、通入控制和其他適當系統。

8.6 SSA 應檢查每一被確定的通入點，包括開敞風雨甲板，並對其被企圖破壞保安的人利用的可能性作出評估。這包括合法進入者和企圖擅自進入者可使用的通入點。

8.7 SSA 應考慮現有保安措施、指導、程序和作業在日常和緊急情況下的繼續相關性並應確定包括下列者的保安指導：

.1 禁區；

.2 火災或其他緊急情況的反應程序；

.3 對船舶人員、旅客、訪問者、商販、修理技工、碼頭工人等等的監控水平；

.4 保安巡邏的頻度和有效性；

.5 通入控制系統，包括識別系統；

.6 保安通信系統和程序；

.7 保安門、屏障和照明；和

.8 如果有的話，保安和監視設備和系統。

8.8 SSA 應考慮應重點保護的人員、活動、業務和作業。這包括：

.1 船舶人員；

.2 旅客、訪問者、商販、修理技工、碼頭設施人員等等；

.3 保持安全航行和應急反應的能力；

.4 貨物，特別是危險品或有害物質；

.5 船舶物料；

.6 如果有的話，船舶保安通信設備和系統；和

.7 如果有的話，船舶保安監視設備和系統。

8.9 SSA 應考慮所有的可能威脅。它們可以包括以下類型的保安事件：

.1 通過爆炸裝置、縱火、搗亂或破壞等方式損壞或損毀船舶或港口設施；

.2 劫持或扣押船舶或船上人員；

.3 破壞貨物、重要船舶設備或系統或船舶物料；

.4 擅自進入或使用，包括出現偷渡者；

.5 走私武器或設備，包括大規模殺傷性武器；

.6 使用船舶運載企圖造成保安事件者和/或其設備；

.7 使用船舶本作為武器或破壞和毀壞的手段；

.8 靠泊或錨泊時從向海側的襲擊；和

.9 海上襲擊。

8.10 SSA 應計及所有可能的弱點，包括：

.1 安全和保安措施間的衝突；

.2 船上職責和保安任務間的衝突；

.3 值班職責、船舶人員的人數，特別是對船員的疲勞、警覺和工作的影響；

.4 任何被查明的保安培訓缺點；和

.5 任何保安設備和系統，包括通信系統。

8.11 CSO 和船舶保安官員（SSO）應始終考慮到保安措施對長期呆在船上的船舶人員的影響。在制定保安措施時，應特別考慮船舶人員的方便、舒適和個人隱私以及其在長時間內保持有效性的能力。

8.12 在完成 SSA 後應準備報告；報告它由評定方法摘要、對評定時發現的每一弱點的陳述以及對解決每一弱點所能使用的對策的陳述構成。應對報告作出保護，防止擅自查閱或洩露。

8.13 如果公司未進行 SSA，則應由 CSO 對 SSA 報告作出檢查和接受。

現場保安檢驗

8.14 現場保安檢驗是任何 SSA 的組成部分。現場保安檢驗應檢查和評估現有的船上保護措施、程序和作業，以：

.1 確保履行所有船上保安職責；

.2 監視禁區，確保只有經授權的人員才能進入；

.3 控制船舶通入，包括任何識別系統；

.4 監視甲板區域和船舶周圍區域；

.5 控制人員及其物品(隨身或寄存的行李和船員個人物品)的上船；

.6 監控貨物的裝卸和船舶物料的交付；和

.7 確保船舶保安通信、信息和設備隨時可用。

9 船舶保安計劃

綜述

9.1 公司保安官員（CSO）有責任確保船舶保安計劃（SSP）的準備和提交供核准。每一各別 SSP 的內容應視其涉及的特定船舶而不同。船舶保安評定（SSA）應指明船舶的特點及潛在的威脅和弱點。制定 SSP 時需對這些特點作出詳述。主管機關可對 SSP 的制定和內容作出建議。

9.2 所有 SSP 均應：

.1 詳述船舶的保安組織結構；

.2 詳述船舶與公司、港口設施、其他船舶和負有保安責任的有關當局的關係；

.3 詳述保障船內和船舶與它船的有效連續通信的通信系統；

.4 詳述應始終就位的 1 級保安的基本保安措施，包括操作和有形措施；

.5 詳述保障船舶及時提升到 2 級保安和（在必要時）3 級保安的額外保安措施；

.6 對定期檢查或審查 SSP 和根據經驗和改變的環境對其作出修正一事作出規定；和

.7 詳述向有關締約政府的聯絡點作出報告的程序。

9.3 制定有效 SSP 的基礎是對與船舶保安相關的所有問題作出徹底評定，包括，特別是，對各個船舶的有形和操作特點（包括航行方式）的透徹了解。

9.4 所有的 SSP 均應由主管機關或其代表核准。如主管機關使用經認可的保安組織（RSO）來檢查或核准 SSP，則該 RSO 不應與制定或幫助制定該計劃的任何其他 RSO 相關。

9.5 CSO 和 SSO 應制定下列者的程序：

.1 評定 SSP 的繼續有效性；和

.2 制定經核准的計劃的修正案。

9.6 SSP 中的保安措施在即將進行對符合第 XI-2 章和本規則第 A 部分的要求的初次核查時應就位。否則不能進行向船舶頒發規定的“國際船舶保安證書”的工作。如果保安設備或系統在此後有任何故障或因任何理由保安措施被中止，則應採用等效的臨時保安措施，將其通知主管機關並得到主管機關的同意。

船舶保安職責的組織和履行

9.7 除 9.2 段中的指導外，SSP 還應確定與所有保安級別相關的下列事項：

.1 有保安任務的所有船上人員的職責和責任；

.2 在所有時刻保持此種連續通信所必需的程序或防護措施；

.3 評定保安程序和任何保安和監視設備和系統的繼續有效性所需的程序，包括設備或系統故障或失靈的識別和反應程序；

.4 保護紙張或電子形式的保安敏感信息的程序和做法；

.5 如果有的話，保安和監視設備和系統的型號和保養要求；

.6 確保及時提交和評定有關可能的破壞保安事件或保安關切事項的報告的程序；和

.7 制定、保持和更新船上的任何危險品或有害物質清單（包括其位置）的程序。

9.8 第 9 節的其餘部分具體陳述了在每一保安級別可採取的有關下列者的保安措施：

.1 船舶人員、旅客、訪問者等的船舶通入；

.2 船上禁區；

.3 貨物裝卸；

.4 船舶物料的交付；

.5 搬運寄存行李；和

.6 監視船舶保安。

船舶通入

9.9 SSP 應制定有關在 SSA 中指明的所有船舶通入裝置的保安措施。這應包括任何：

.1 出入梯；

.2 出入通道；

.3 出入坡道；

.4 出入門、舷窗、窗子和孔口；

.5 繫泊纜和錨鏈；和

.6 起重機和吊具。

9.10 對其中每一裝置，SSP 應指明在每一保安級別使用限止或禁止通入的適當位置。SSP 應對每一保安級別確定限制或禁止的類型及執行方法。

9.11 SSP 應為每一保安級別確定允許進入船舶和無質疑地讓人員留在船上所需的識別方法。這可能涉及制定一種計及分別用於船舶人員和訪問者的永久和臨時識別的適當識別系統。在可行時，任何船舶識別系統均應與使用於港口設施者作出協調。旅客應能使用登船卡、船票等證明其身份，但不准進入禁區，除非得到監控。SSP 應制定規定，確保對識別系統作出定期更新和對濫用程序採取紀律行動。

9.12 在要求時不願意或不能夠證實其身份和/或證實其訪問目的人員應被拒絕進船並應視情將其上船企圖報告 SSO、CSO、港口設施保安官員(PFSO)和負有保安責任的國家或地方當局。

9.13 SSP 應確定實施任何通入控制的頻度，尤其是對隨機或偶爾實施者。

1 級保安

9.14 在 1 級保安時，SSP 應確定控制船舶通入的保安措施。可實施以下保安措施：

.1 核查要上船的所有人員的身份並通過核查諸如加入指令、旅客船票、登船卡、工作命令等核實其上船理由；

.2 船舶應與港口設施合作，確保設立了專用的安檢區，對人員、行李（包括隨身物品）、個人物品、車輛及其裝載物進行檢查和搜查；

.3 船舶應與港口設施合作，確保按 SSP 規定的頻度在裝船前對要裝上車輛運輸船、滾裝和其他客船的車輛進行搜查；

.4 將經核查的人員及其個人物品與未經核查的人員及其個人物品分開；

.5 將上船旅客與下船旅客分開；

.6 指明應予關閉或應有人照看的通入點，以防止擅自進入；

.7 通過鎖或其他裝置關閉與旅客和訪問者使用區域相鄰的無人處所的通道；和

.8 向所有船舶人員提供有關可能威脅、報告可疑人員、物體或活動的程序和提高警惕的必要性的保安簡報。

9.15 在 1 級保安時，要上船的所有人員均應接受搜查。包括隨機搜查在內的此種搜查的頻度應在經核准的 SSP 中指明並應得到主管機關的特別核准。此種搜查最好由港口設施在船舶的密切配合下在船舶附近進行。除非有明確理由這樣做，否則不應要求船舶人員的成員搜查其同事或同事的個人物品。任何此種搜查均應充分計及各個人員的人權並維護其基本的人的尊嚴。

2 級保安

9.16 在 2 級保安時，SSP 應確定用以防範保安事件的更大風險的保安措施，確保更高的警惕和更嚴格的控制。它們可以包括：

.1 在寂靜時間指派額外人員對甲板區域進行巡邏，防止擅自進入；

.2 限制船舶通入點的數目，指明應予關閉的通入點及其適當的關閉裝置；

.3 防止從水側進入船舶，包括例如與港口設施合作、提供船舶巡邏；

.4 在港口設施的密切配合下在船舶的岸側建立禁區；

.5 增加對要上船或被裝船的人員、個人物品和車輛的搜查頻度和詳細度；

.6 監護船上的訪問者；

.7 向所有船舶人員提供有關任何被確定的威脅、重申報告可疑人員、物品或活動的程序和強調要有更高警惕的額外的具體保安簡報；和

.8 進行全面或局部的船舶搜查。

3 級保安

9.17 在 3 級保安時，船舶應遵守保安事件或其威脅的反應人員發出的指示。SSP 應詳述船舶在反應人員和港口設施的密切配合下能夠採取的保安措施。它們可以包括：

.1 將通入限制在一個單一的、有控制的通入點；

.2 僅允許保安事件或其威脅的反應人員進入；

.3 指導船上人員；

.4 中止上船或下船；

.5 中止貨物裝卸作業、交付等等；

.6 撤離船舶；

.7 船舶運動；和

.8 做好全面或局部搜查船舶的準備。

船上禁區

9.18 SSP 應指明要在船上設立的禁區，說明其範圍、實施時間、要採取的控制進入禁區和控制禁區內的活動的保安措施。禁區的目的是：

.1 防止擅自進入；

.2 保護旅客、船舶人員和被允許上船的港口設施或其他機構的人員；

.3 保護船內的保安敏感區域；和

.4 防止貨物和船舶物料被破壞。

9.19 SSP 應確保有明確的政策和做法來控制對所有禁區的進入。

9.20 SSP 應規定對所有禁區作出明顯標態，指出進入該區域是有限制的，擅自出現在該區域內是破壞保安。

9.21 禁區可包括：

.1 駕駛台、A 類機器處所或第 II-2 章規定的其他控制站；

.2 有保安和監視設備和系統及其控制裝置和照明系統控制裝置的處所；

.3 通風和空調系統和其他類似處所；

.4 通達移動水箱、泵或歧管的處所；

.5 有危險品或有害物質的處所；

.6 有貨泵及其控制裝置的處所；

.7 貨物處所和有船舶物料的處所；

.8 船員居住區；和

.9 CSO 通過 SSA 確定的為維護船舶保安而必須對進入作出限制的任何其他區域。

1 級保安

9.22 在 1 級保安時，SSP 應確定對禁區使用的保安措施。它們可以包括：

.1 鎖閉或關閉通入點；

.2 使用監視設備監視該區域；

.3 使用警衛或巡邏；和

.4 使用自動侵入探測裝置向船舶人員發出擅自進入的警戒。

2 級保安

9.23 在 2 級保安時，應增加監視和控制禁區通入的頻度和強度，確保只有經許可的人員進入。SSP 應確定要使用的額外措施。它們可以包括：

.1 在通入點相鄰處設立禁區；

.2 連續監視監視設備；和

.3 派額外人員守護和巡邏禁區。

3 級保安

9.24 在 3 級保安時，船舶應遵守保安事件或其威脅的反應人員發出的指示。SSP 應詳述船舶在反應人員和港口設備的密切配合下能夠採取的保安措施。它們可以包括：

.1 在保安事件或在據信的保安威脅地點附近設立額外的船上禁區，不准進入；

.2 將搜查禁區作為搜查船舶的組成部分。

貨物裝卸

9.25 貨物裝卸的保安措施應：

.1 防止破壞；和

.2 防止在船上接受和存放不供運載的貨物。

9.26 某些保安措施必須在港口設施的配合下實施。保安措施應包括在船舶通入點處的清單控制程序。貨物一旦裝船即應能確定是經准許裝船的。此外，制定的保安措施應確保貨物在裝船後不被破壞。

1 級保安

9.27 在 1 級保安時，SSP 應確定貨物裝卸期間使用的保安措施。它們可以包括：

.1 在貨物裝卸作業之前和之時對貨物、貨物運輸單元和貨物處所的日常核查；

.2 旨在確保裝船的貨物與貨物單證相符的核查；

.3 在港口設備的配合下確保按 SSP 規定的頻度在裝船前對要裝上車輛運輸船、滾裝船和客船的車輛進行搜查；和

.4 核查封條或用以防止破壞的其他方法。

9.28 可以下列方法進行貨物核查：

.1 外觀和物理檢查；

.2 使用掃瞄/探測設備、機械裝置或狗。

9.29 在有經常或重複的貨物運動時，CSO 或 SSO 經與港口設施協商，可與發貨人或對此種貨物負責的其他人員議定有關場地外核查、密封、時間表、證件等等的安排。此種安排應通知有關的 PFSO 並得到其同意。

2 級保安

9.30 在 2 級保安時，SSP 應確定在貨物裝卸期間使用的額外保安措施。它們可以包括：

.1 對貨物、貨物運輸單元和貨物處所的詳細核查；

.2 確保只有預定貨物被裝船的強化核查；

.3 對要裝上車輛運輸船、滾裝船和客船的車輛的強化核查；和

.4 對封條或用於防止破壞的其他方法的更頻繁和詳細的核查。

9.31 可以下列方法進行詳細的貨物核查：

.1 增加外觀和物理檢查的頻度和詳細度；

.2 增加使用掃瞄/探測設備、機械裝置或狗的頻度；和

.3 按達成的協議和程序與發貨人或其他負責方協調強化的保安措施。

3 級保安

9.32 在 3 級保安時，船舶應遵守保安事件或其威脅的反應人員發出的指示。SSP 應詳述船舶在反應人員和港口設施的密切配合下能夠採取的保安措施。它們可以包括：

.1 中止貨物裝卸；和

.2 核查，如果有的話，船上運載的危險品和有害物質的清單和位置。

船舶物料交付

9.33 有關船舶物料交付的保安措施應：

.1 確保對船舶物料和包裝完整性作出核查；

.2 防止接受未經檢查的船舶物料；

.3 防止破壞；和

.4 防止接受未定購的船舶物料。

9.34 對於經常使用港口設施的船舶，制定涉及船舶、其供應商和港口設施的有關交貨通知和時間及證件的程序可能是適當的。應始終有某種辦法證實交付的物料附有它們係船舶定購者的證明。

1 級保安

9.35 在 1 級保安時，SSP 應確定在船舶物料交付期間使用的保安措施。它們可以包括：

.1 在裝船前進行確保物料與定單相符的核查；和

.2 確保船舶物料的立即保安貯存。

2 級保安

9.36 在 2 級保安時，SSP 應確定在船舶物料交付期間使用的額外保安措施，在船上接受物料前進行核查並加強檢查。

3 級保安

9.37 在 3 級保安時，船舶應遵守保安事件或其威脅的反應人員發出的指示。SSP 應詳述船舶在反應人員和港口設施的密切配合下能夠採取的保安措施。它們可以包括：

.1 對船舶物料進行更廣泛的核查；

.2 作好限制或中止船舶物料裝卸的準備；和

.3 拒絕接受船舶物料上船。

寄存行李的搬運

9.38 SSP 應確定要使用的保安措施，確保在對寄存行李（即在檢查和搜查時不在旅客或船舶人員身邊的任何行李，包括個人物品）作出識別和適當檢查（包括搜查）後才准其上船。並非要此種行李將接受船舶和港口設施雙方的檢查。在雙方都有適當設備時，檢查責任應由港口設施承擔。與港口設施的密切配合是必要的，應採取步驟確保在檢查後對寄存行李作出保安的搬運。

1 級保安

9.39 在 1 級保安時，SSP 應確定在搬運寄存行李時使用的保安措施，確保對寄存行李進行高達並包括 100%的檢查或搜查。它們可以包括使用 X 光檢查。

2 級保安

9.40 在 2 級保安時，SSP 應確定在搬運寄存行李時使用的額外保安措施。它們應包括對所有寄存行李的 100%的 X 光檢查。

3 級保安

9.41 在 3 級保安時，船舶應遵守保安事件或其威脅的反應人員發出的指示。SSP 應詳述船舶在反應人員和港口設施的密切配合下能夠採取的保安措施。它們可以包括：

.1 對此種行李進行更全面的檢查，如從至少兩個不同角度對其使用 X 光；

.2 做好限制或中止搬運寄存行李的準備；和

.3 拒絕接受寄存行李上船。

監視船舶保安

9.42 船舶應有監視船舶、船上禁區和船舶周圍區域的能力。此種監視能力可包括使用：

.1 照明；

.2 值班人員、警衛和甲板值班，包括巡邏；和

.3 自動侵入探測裝置和監視設備。

9.43 使用時，自動侵入探測裝置應啓動在連續看守或監視位置上的聲響和/或視覺警報。

9.44 SSP 應確定每一保安級別時需要的程序和設備和確保監測設備能連續工作的方法，包括考慮到天氣狀況或電力中斷的可能影響。

1 級保安

9.45 在 1 級保安時，SSP 應確定要使用的保安措施，它們可以是照明、值班人員、警衛或使用保安和監視設備的某種組合，使船舶保安人員能對船舶，特別是屏障和禁區，作出觀察。

9.46 必要時，在黑暗和低能見度期間，當進行船/港界面活動或當船舶在港口或錨地時，應對船舶甲板和船舶通入點作出照明。必要時，在航行期間，船舶應使用與安全航行相符的最大現有照明並考慮到現行的《國際海上避碰規則》的規定。在確定照明的適當程序和位置時，應考慮到以下者：

.1 船舶人員應能發現船外的岸側和水側活動；

.2 照明範圍應包括船上和船舶周圍區域；

.3 照明範圍應便利在通入點上的人員識別；和

.4 可通過與港口設施的協調來提供照明範圍。

2 級保安

9.47 在 2 級保安時，SSP 應確定加強監測和監視能力的額外保安措施。它們可以包括：

.1 增加保安巡邏的頻度和詳細度；

.2 增加照明範圍和強度或增加保安和監視設備的使用；

.3 指派額外人員作為保安瞭望員；和

.4 確保與水側船舶巡邏和岸側徒步和車輛巡邏的協調。

9.48 可能需要額外照明以防範保安事件的更大風險。必要時，可通過與港口設施協調提供額外的岸側照明來達到額外照明要求。

3 級保安

9.49 在 3 級保安時，船舶應遵守保安事件或其威脅的反應人員發出的指示。SSP 應詳述船舶在反應人員和港口設施的密切配合下能夠採取的保安措施。它們可以包括：

.1 打開船上的所有照明或對船舶附近區域予以照明；

.2 打開能記錄船上或船舶附近活動的所有船上監視設備；

.3 使此種監視設備的連續記錄時間最大化；

.4 做好在水下檢查船體的準備；和

.5 啓動防止從水下潛到船體的措施，如果可行，應包括降低船舶推進器的轉速。

不同保安級別

9.50 SSP 應制定在船舶保安級別高於對港口設施使用者時船舶能採用的程序和保安措施的細節。

本規則未涉及的活動

9.51 SSP 應制定在下列情況下船舶應使用的程序和保安措施的細節：

.1 它在非締約政府的國家的港口中；

.2 它在與本規則不適用的某一船舶進行界面；

.3 它在與固定或浮動平台或就位的移動式鑽井裝置進行界面；或

.4 它在與不需要符合第 XI-2 章和本規則第 A 部分的港口或港口設施進行界面。

保安聲明

9.52 SSP 應詳述如何處理港口設施的“保安聲明”要求和在何種情況下船舶本身應要求 DoS。

審核和檢查

9.53 SSP 應確定 CSO 和 SSO 審核 SSP 的繼續有效性的方法和在檢查、更新或修正 SSP 時就遵守的程序。

10 記錄

綜述

10.1 應向締約政府正式授權官員提供各種記錄，以證實船舶保安計劃的規定正在得到實施。

10.2 記錄可以任何格式作出，但應有防止擅自查閱或洩露的保護。

11 公司保安官員

有關指導載於 8、9 和 13 節中。

12 船舶保安官員

有關指導載於 8、9 和 13 節中。

13 船舶保安培訓、操練和演習

培訓

13.1 公司保安官員（CSO）和適當的岸上公司人員及船舶保安官員（SSO）應視情在以下某些或所有方面具有知識或接受培訓：

.1 保安管理；

.2 有關國際公約、規則和建議書；

.3 有關政府立法和規則；

.4 其他保安組織的責任和職能；

.5 船舶保安評定方法；

.6 船舶保安檢驗和檢查方法；

.7 船舶和港口的作業和狀況；

.8 船舶和港口設施保安措施；

.9 應急防備和反應及應急規劃；

.10 保安培訓和教育的講授技巧，包括保安措施和程序；

.11 處理敏感的保安信息和保安通信；

.12 對當前的保安威脅和方式的知識；

.13 對武器、危險物質和裝置的識別和探測；

.14 在無歧視的基礎上對可能威脅保安的人員的特點和行為方式的識別；

.15 逃避保安措施使用的技術；

.16 保安設備和系統及其操作局限；

.17 進行審核、檢查、控制和監視的方法；

.18 有形搜查和非侵入檢查的方法；

.19 保安操練和演習，包括與港口設施的操練和演習；和

.20 對保安操練和演習的評定。

13.2 此外，SSO 應視情在以下某些或所有方面具有適當知識和接受培訓：

.1 船舶佈局；

.2 船舶保安計劃和有關程序（包括以情況為基礎的反應方法培訓）；

.3 人群管理和控制技術；

.4 保安設備和系統的操作；和

.5 保安設備和系統的測試、校準和海上保養。

13.3 負有具體保安職責的船舶人員應具有履行指定職責的足夠知識和能力，視情包括：

.1 對當前的保安威脅和方式的知識；

.2 對武器、危險物質和裝置的識別和探測；

.3 對可能威脅保安的人員的特點和行為方式的識別；

.4 逃避保安措施使用的技術；

.5 人群管理和控制技術；

.6 保安通信；

.7 對緊急程序和應急計劃的知識；

.8 保安設備和系統的操作；

.9 保安設備和系統的測試、校準和海上保養；

.10 檢查、控制和監測技術；

.11 人員、個人物品、行李、貨物和船舶物料的有形搜查的方法。

13.4 所有其他船上人員均應足夠地了解並熟悉船舶保安計劃（SSP）的有關規定，包括：

.1 不同保安級別的意義和相應要求；

.2 對應急程序和應急計劃的知識；

.3 對武器、危險物質和裝置的識別和探測；

.4 在無歧視的基礎上，對有可能威脅保安的人員的特點和行為方式的識別；和

.5 逃避保安措施使用的技術。

操練和演習

13.5 操練和演習的目的是確保船上人員精通所有保安級別的所有指定保安職責，查明需要處理的任何保安缺陷。

13.6 為確保船舶保安計劃的規定得到有效實施，應至少每三個月舉行一次操練。此外，在每次船上的人員變動超過百分之 25 並有在前三個月內未曾參加船上的任何操練的人員時，應在變動後的一個星期內進行操練。這些操練應檢驗計劃的各個成分，如 8.9 段中列出的那些保安威脅。

13.7 各種類型的演習可包括船舶保安官員和，如果有的話，公司保安官員、港口設施保安官員、締約政府有關當局的參與，應在每日曆年度至少進行一次，且演習間隔不應超過 18 個月。這些演習應檢驗通信、協調、資源配備和反應。這些演習可以是：

.1 真實或實況的；

.2 桌面模擬或研討會；或

.3 與舉行的其他演習，如搜救或應急反應演習，結合在一起。

13.8 公司參與另一締約政府的演習應得到主管機關的承認。

14 港口設施保安

有關指導載於 15、16 和 18 節中。

15 港口設施保安評定

綜述

15.1 港口設施保安評定（PFSA）可由經認可的保安組織（RSO）進行。但對完成的 PFSA 的核准應由有關締約政府作出。

15.2 如果締約政府使用 RSO 來檢查或核查對 PFSA 的符合，則該 RSO 不應與制定或幫助制定該評定的任何其他 RSO 相關。

15.3 PFSA 應闡述港口設施內的以下要素：

.1 有形保安；

.2 結構完整性；

.3 人員保護系統；

.4 程序政策；

.5 無線電和電信系統，包括電腦系統和網絡；

.6 有關的運輸基礎設施；

.7 公共設施；和

.8 在受到損壞或用於非法觀察時可能對港口設施內人員、財產或作業造成風險的其他區域。

15.4 參與 PFSA 的人員應能在以下方面獲得專家幫助：

.1 對當前保安威脅和方式的知識；

.2 對武器、危險物質和裝置的識別和探測；

.3 在無歧視的基礎上對可能威脅保安的人員的特點和行為方式的識別；

.4 逃避保安措施使用的技術；

.5 造成保安事件使用的方法；

.6 爆炸品對結構和港口設施業務的影響；

.7 港口設施保安；

.8 港口業務做法；

.9 應急規劃、應急防備和反應；

.10 有形保安措施，如柵欄；

.11 無線電和電信系統，包括電腦系統和網絡；

.12 運輸和土木工程；和

.13 船舶和港口作業。

對重點保護的重要資產和基礎設施的確定和評估

15.5 重要資產和基礎設施的確定和評估是一項因此確定各種結構和裝置對港口職能的相對重要性的工作。該確定和評估工作是重要的，因為它為將防範戰略聚集於更需要防範保安事件的那些資產和結構提供了基礎。該工作應計及潛在的喪生、港口的經濟意義、象徵價值和是否有政府裝置。

15.6 應使用資產和基礎設施的確定和評估來確定其在保護上的相對重要性的優先順序。主要的關切應是避免死亡或受傷。還需考慮在沒有該資產時港口設施、結構或裝置能否繼續工作以及迅速恢復正常工作的可能程度。

15.7 視為需重點保護的資財和基礎設施可包括：

.1 通道、入口、進口航道及錨地、操縱和靠泊區；

.2 貨物設施、碼頭、貯藏區和貨物裝卸設備；

.3 配電系統、無線電和電信系統、電腦系統和網絡之類的系統；

.4 港口船舶交通管理系統和助航裝置；

.5 發電站、貨物輸送管和供水裝置；

.6 橋樑、鐵路、道路；

.7 港口服務船，包括引航船、拖輪、港口駁船等等；

.8 保安和監視設備和系統；和

.9 港口設施的鄰近水域。

15.8 資產和基礎設施的明確確定對於評估港口設施的保安要求、確定保護措施的優先順序和旨在對港口設施作出更好保護的資源分配決定是必要的。該工作可能涉及與有關當局就港口設施附近能造成設施內損壞或能用於造成設施損壞、對設施的非法觀察或分散注意力的結構進行磋商。

確定對資產和基礎設施的可能威脅及其發生可能性以確定保安措施及其優先順序

15.9 應確定威脅資產和基礎設施保安的可能行為和進行這些行為的方法，以便對某一特定資產或地點在保安事件方面的弱點作出評定，確定保安要求及其優先順序，從而作出規劃和資源分配。對每一潛在行為及其方法的確定和評估應基於各種因素，包括政府機構的威脅評定。通過確定和評定威脅，評定人員不必依據最壞案例的情況來指導規劃和資源分配。

15.10 PFSA 應包括在與有關國家保安組織協商下作出的、用以確定以下者的評定：

.1 使港口設施可能成為襲擊目標的任何港口設施特定事項，包括使用該設施的船舶交通；

.2 襲擊港口和在港口襲擊在喪生、財產損壞和包括運輸系統中斷在內的經濟中斷等方面的可能後果；

.3 可能發動此種襲擊者的能力和意圖；和

.4 可能的襲擊形式，

從而作出對必需制定保安措施予以防範的風險程度的全面評定。

15.11 PFSA 應考慮到所有可能威脅。它們可以包括以下類型的保安事件：

.1 損壞或毀壞港口設施或船舶，如通過爆炸裝置、縱火、搗亂或破壞；

.2 劫持或扣押船舶或船上人員；

.3 破壞貨物、必要的船舶設備或系統或船舶物料；

.4 擅自進入或使用，包括有偷渡者；

.5 走私武器或設備，包括大規模死傷性武器；

.6 使用船舶運載企圖造成保安事件的人員及其設備；

.7 使用船舶本身作為造成損壞或毀壞的武器或手段；

.8 封鎖港口入口、船閘、進港航道等；和

.9 核、生物和化學襲擊。

15.12 該工作應涉及與有關當局就港口設施附近能造成設施內損壞或能用於造成設施損壞、對設施的非法觀察或分散注意力的結構進行磋商。

對策的確定、選擇和優先順序化和程序改變及其對減少弱點的有效程度

15.13 對策的確定和優先順序化旨在確保使用最有效的保安措施來減少港口設施或船/港界面在可能襲擊方面的弱點。

15.14 應根據它們是否減少襲擊概率之類的因素來選擇保安措施，並應使用包括下列者的信息對其作出評估：

.1 保安檢驗、檢查和審核；

.2 與港口設施的所有人和經營人和，如適當，相鄰結構的所有人/經營人的磋商；

.3 保安事件的歷史資料；和

.4 港口設施內的作業。

確定弱點

15.15 確定有形結構、人員保護系統、工作或可能引起保安事件的其他方面的弱點可被用於制定消除或降低這些弱點的選擇辦法。例如，分析可能揭示出可通過有形措施，如永久屏障、警報器、監視設備等，予以解決的港口設施保安系統或諸如供水裝置、橋樑等未受保護的基礎設施的弱點。

15.16 確定弱點應包括對下列事項的考慮：

.1 港口設施及在設施中靠泊的船舶的水側和岸側通道；

.2 碼頭、設施和相關結構的結構完整性；

.3 現有的保安措施和程序，包括識別系統；

.4 港口業務和公共設施的現有保安措施和程序；

.5 保護包括電腦系統和網絡在內的無線電和電信設備、港口業務和公共設施的措施；

.6 在襲擊時或為襲擊目的可被利用相鄰區域；

.7 與提供水側/岸側保安業務的私營保安公司的現有協議；

.8 安全和保安措施和程序間的任何衝突政策；

.9 任何衝突的港口設施和保安職責安排；

.10 任何執行和人員限制；

.11 在培訓和操練時查明的任何不足；和

.12 在事件或警戒、保安關切事項報告、控制措施的執行、審核等等之後，在日常作業中查明的任何不足。

16 港口設施保安計劃

綜述

16.1 準備港口設施保安計劃(PFSP)是港口設施保安官員(PFSO)的責任。雖然 PFSO 不必親自執行與其職務相關的所有職責，但確保這些職責得到正確履行的最後責任仍由各個 PFSO 承擔。

16.2 每一 PFSP 的內容應視其所涉及的港口設施的特定情況而有所不同。港口設施保安評定（PFSA）指明了引起任命 PFSO 和準備 PFSP的必要的港口設施和潛在風險的特點。準備 PFSP時需要在 PFSP 中闡述這些特點和其他的地方或國家保安考慮事項並制定適當保安措施使破壞保安的可能性和潛在風險的後果最小化。締約政府可對 PFSP 的制定和內容作出建議。

16.3 所有的 PFSP 均應：

.1 詳述港口設施的保安組織；

.2 詳述該組織與其他有關當局的聯繫和保障該組織的有效連續運作及其與包括港內船舶在內的其他方面的聯繫的必要通信系統；

.3 詳述將就位的基本 1 級保安措施，包括操作和有形措施；

.4 詳述保障港口設施及時升至 2 級保安和，在必要時，3 級保安的額外保安措施；

.5 對 PFSP 的定期檢查或審核和對其因應經驗和改變的情況的修正作出規定；

.6 詳述向適當的締約政府聯絡點作出報告的程序。

16.4 準備有效的 PFSP 需要對保安的所有有關事項作出徹底的評定，包括尤其是對各港口設施的有形和操作特點的透徹了解。

16.5 締約政府應對在其管轄範圍內的港口設施的 PFSP 作出核准。締約政府應制定用以評定每一 PFSP 是否繼續有效的程序並可在初次核准前或核准後對 PFSP 作出修正。PFSP 應為保留保安事件和威

務、檢查、審核、培訓、操作和演習的記錄以作為符合這些要求的證據一事作出準備。

16.6 PFSP 中的保安措施應在 PFSP 被核准後的一個合理期限內就位。PFSP 應確定每一措施在何時就位。如果在提供措施方面可能會有任何拖延，則應與負責核准該 PFSP 的締約政府就此進行討論。令人滿意的、提供同等保安程度的替代臨時保安措施應得到同意，供在任何臨時期限內實施。

16.7 在船上或船舶附近和在港口設施中使用武器可能會有特別和重大的安全風險，特別是對於某些危險或有害物質，因此應給與非常仔細的考慮。如果締約政府決定必需在這些區域內使用武裝人員，則該締約政府應確保這些人員在使用武器上得到正式授權和培訓，確保他們認識到這些區域內的具體安全風險。如果締約政府授權使用武器，則應頒發有關其使用的具體安全指南。PFSP 應載有有關該事宜的具體指導，特別是其對運載危險品或有害物質的船舶的影響。

港口設施保安職責的組織和履行

16.8 除 16.3 段中的指導外，PFSP 還應確定與所有保安級別有關的下列事項：

.1 港口設施保安組織的任務和結構；

.2 所有負有保安任務的港口設施人員的職責、責任和培訓要求以及對各個人員的工作成效作出評定所需的工作評定方法；

.3 港口設施保安組織與負有保安責任的其他國家或地方當局的聯繫；

.4 為保障港口設施保安人員、港內船舶和，在適當時，負有保安責任的國家或地方當局間的有效和連續通信提供的通信系統；

.5 保障在所有時刻保持此種連續通信所必需的程序或保護措施；

.6 保護紙張或電子形式的保安敏感信息的程序和做法；

.7 評定保安措施、程序和設備的繼續有效性的程序，包括對設備失靈或故障的識別和反應；

.8 提交和評定有關可能的破壞保安事件或保安關切事項的報告的程序；

.9 貨物裝卸程序；

.10 船舶物料交付程序；

.11 保管和更新危險品和有害物質及其在港口設施內的位置的記錄的程序；

.12 向水側巡邏隊和專家搜查隊報警和獲得其服務的程序，包括炸彈搜查和水下搜查；

.13 在有此要求時，幫助船舶保安官員確認要上船人員的身份的程序；和

.14 便利船舶人員的登岸假或人員變動以及包括船員福利和勞工組織的代表在內的訪問者上船的程序。

16.9 第 16 節的其餘部分具體地闡述了在每一保安級別時可以採取的有關下列事項的保安措施：

.1 港口設施的通入；

.2 港口設施內的禁區；

.3 貨物裝卸；

.4 船舶物料的交付；

.5 搬運寄存行李；和

.6 監視船舶設施的保安。

港口設施的通入

16.10 PFSP 應確定 PFSA 中指明的所有港口設施通道的保安措施。

16.11 對於每一通道，PFSP 應指明在每一保安級別應使用通入限制或禁止的適當位置。對於每一保安級別，PFSP 應對使用的限制或禁止類型以及執行方法作出規定。

16.12 PFSP 應為每一保安級別確定允許進入港口設施和無質疑地讓人員留在港口設施內所需的識別方法。這可能需要制定一種計及分別用於港口人員和訪問者的永久和臨時識別的適當識別系統。在可行時，任何港口設施識別系統均應與經常使用該港口設施的船舶所使用者協調。旅客應能使用登船卡、船票等來證明其身份，但不准進入禁區，除非得到監控。PFSP 應制定規定，確保對識別系統作出定期更新和對濫用程序採取紀律行動。

16.13 在要求時不願意或不能夠證實其身份和/或證實其訪問目的人員應被拒絕進入港口設施並應將他們的進入企圖報告給 PFSO 和負有保安責任的國家或地方當局。

16.14 PFSP 應指明要進行人員、個人物品和車輛搜查的位置。不論當時的天氣狀況如何，均應按 PFSP 中規定的頻度對此種位置作出遮閉，以便利連續作業。在接受搜查後，人員、個人物品和車輛應直接進入有限制的等候、登乘或裝車區域。

16.15 PFSP 應為經核查和未經核查的人員及個人物品設定分開的區域；如果可能，為上船/下船旅客、船舶人員及其個人物品設定分開的區域，確保未核查的人員無法與經核查的人員接觸。

16.16 PFSP 應確定任何通入控制的實施頻度，特別是在隨機或偶爾實施此種控制時。

1 級保安

16.17 在 1 級保安時，PFSP 應確定可實施下列保安措施的控制點：

.1 禁區。它應按締約政府核准的標準在周圍裝有隔柵或屏障；

.2 核查與船舶有關的、要進入港口設施的所有人員的身份，包括旅客、船舶人員和訪問者，通過核查諸如加入指令、旅客船票、登船卡、工作命令等核實其進港理由；

.3 核查與船舶有關的、要進入港口設施的人員使用的車輛；

.4 核查港口設施人員和港口設施內的僱用人員的身份及其車輛；

.5 限制進入。在不能確定其身份時，不准港口設施未僱用或不在港口設施中工作的人員進入；

.6 搜查人員、個人物品、車輛及其裝載物；和

.7 指明不經常使用的任何通入點。它們應被長期關閉和鎖閉。

16.18 在 1 級保安時，要進入港口設施的所有人員均應接受搜查。包括隨機搜查在內的此種搜查的頻度所在經核准的 PFSP 中指明並應得到締約政府的特別核准。除非有明確理由這樣做，否則不應要求船舶人員的成員搜查其同事或同事的個人物品。任何此種搜查均應充分計及各個人員的人權並維護其基本的人的尊嚴。

2 級保安

16.19 在 2 級保安時，PFSP 應確定應使用的額外保安措施。它們可以包括：

.1 指定額外人員守護通入點並巡查周圍的屏障；

.2 限制港口設施通入點的數目，指明應予關閉的通入點及其適當的關閉裝置；

.3 準備阻止通過其餘通入點的運動的裝置，如保安屏障；

.4 增加搜查人員、個人物品和車輛的頻度；

.5 不准不能提供要進入港口設置的可核實的理由的訪問者進入；和

.6 使用巡邏艇加強水側保安。

3 級保安

16.20 在 3 級保安時，港口設施應遵守保安事件或其威脅的反應人員發出的指示。PFSP 應詳述港口設施在反應人員和港口設施中的船舶的密切配合下能夠採取的保安措施。它們可以包括：

.1 中止對港口設施全部或局部範圍的進入；

.2 僅允許保安事件或其威脅的反應人員進入；

.3 中止在港口設施全部或局部範圍內的徒步或車輛運動；

.4 如適當，增加港口設施內的保安巡邏；

.5 中止港口設施全部或局部範圍內的港口作業；

.6 指揮港口設施全部或局部範圍內的船舶運動；和

.7 港口設施的全部或局部撤離。

港口設施內的禁區

16.21 PFSP 應指明要在港口設施內設立的禁區，說明其範圍、實施時間、要採取的控制禁區通入和控制禁區內的活動的保安措施。在適當的情況下還應包括確保在設立臨時禁區之前和之後對其作出保安檢查的措施。禁區的目的是：

.1 保護旅客、船舶人員、港口設施人員和訪問者，包括船舶的訪問者；

.2 保護港口設施；

.3 保護使用港口設施和為其服務的船舶；

.4 保護港口設施內的保安敏感位置和區域；

.5 保護保安和監視設備和系統；和

.6 防止貨物和船舶物料被破壞。

16.22 PFSP 應確保所有禁區均有明確的保安措施來控制：

.1 人員通入；

.2 車輛的進入、停放和裝卸；

.3 貨物和船舶物料的運動和貯藏；和

.4 寄存的行李或個人物品。

16.23 PFSP 應規定對所有禁區作出清晰標誌，指出進入該區域是有限制的，擅自出現在該區域內是破壞保安。

16.24 在裝有自動侵入探測裝置時，它們應向能對警報的觸發作出反應的制控中心發出警戒。

16.25 禁區可包括：

.1 與船舶相鄰的岸側和水側區域；

.2 上下船區域、旅客和船舶人員的等候和處理區域，包括搜查點；

.3 貨物和物料的裝卸或貯藏區域；

.4 包括貨物單證在內的保安敏感信息的存放位置；

.5 危險品和有害物質的存放區域；

.6 船舶交通管理制度控制室、航標和港口控制樓，包括保安和監視控制室；

.7 存放或安裝保安和監視設備的區域；

.8 必要的電氣、無線電和電信、水或其他公共設施；和

.9 應對船舶、車輛和人員的通入作出限制的港口設施內的其他位置。

16.26 經有關當局同意，可將保安措施擴大到限制可對港口設施進行觀察的結構的擅自進入。

1 級保安

16.27 在 1 級保安時，PFSP 應確定使用於禁區的保安措施。它們可以包括：

.1 提供永久或臨時屏障包圍禁區。其標準應得到締約政府的接受；

.2 提供在使用時可由警衛控制通入、在不使用時可有效鎖閉或閂閉的通入點；

.3 提供必須出示的、用以證明該人員有權在禁區內的通行證；

.4 對允許進入禁區的車輛作出清晰標誌；

.5 提供警衛和巡邏；

.6 提供自動侵入探測裝置或監視設備或系統來探測擅自進入禁區或禁區內的運動；和

.7 控制使用港口設施的船舶附近的船舶運動。

2 級保安

16.28 在 2 級保安時，PFSP 應確定監視和控制禁區通入的更高頻度和強度。PFSP 應確定額外保安措施。它們可以包括：

.1 提高禁區周圍的屏障或柵欄的有效性，包括使用巡邏或自動侵入探測裝置；

.2 減少禁區通入點的數目，加強對其餘通道的控制；

.3 對在靠泊船舶附近停車作出限制；

.4 進一步限制禁區的通入和禁區內的運動和貯藏；

.5 使用被連續監測和記錄的監視設備；

.6 增加在禁區邊界和禁區內的巡邏的數量和頻度，包括水側巡邏；

.7 在禁區附近設立限制通入的區域；和

.8 對未經授權的船舶進入使用港口設施的船舶的鄰近水域作出限制。

3 級保安

16.29 在 3 級保安時，港口設施應遵守保安事件或其威脅的反應人員發出的指示。PFSP 應詳述港口設施在反應人員和港口設施內的船舶的密切配合下能夠採取的保安措施。它們可以包括：

.1 在保安事件或據信的保安威脅地點附近設立額外的港口設施內禁區，不准進入；和

.2 作好搜查禁區的準備，將其作為搜查港口設施全部或局部區域的組成部分。

貨物裝卸

16.30 貨物裝卸的保安措施應：

.1 防止破壞；

.2 防止在港口設施內接受和存放不供運載的貨物。

16.31 保安措施應包括在港口設施通入點處的清單控制程序。貨物一旦在港口設施內，即應能確定是已作出核查並被接受裝船或在裝船前暫時存放在禁區中。對沒有經確認的裝船日期的貨物進入港口設施作出限制可能是適當的。

1 級保安

16.32 在 1 級保安時，PFSP 應確定在貨物裝卸期間使用的保安措施。它們可以包括：

.1 在貨物裝卸作業之前和之時對港口設施內的貨物、貨物運輸單元和貨物存放區域的日常核查；

.2 旨在確保進入港口設施的貨物與交運通知書或等同的貨物單證相符的核查；

.3 船舶搜查；和

.4 核查封條和防止貨物在進入港口設施和存放在港口設施中時受到破壞而使用的其他方法。

16.33 可使用某些或全部下列方法進行貨物核查：

.1 外觀或物理檢查；

.2 使用掃瞄/探測設備、機械裝置或狗。

16.34 在有經常或重複的貨物運動時，CSO 或 SSO 經與港口設施協商，可與發貨人或對此種貨物負責的其他人員議定有關船邊核查、密封、時間表、證件等等的安排。此種安排應通知有關的 PFSO 並得到其同意。

2 級保安

16.35 在 2 級保安時，PFSP 應確定在貨物裝卸期間使用的加強控制的額外保安措施。它們可以包括：

.1 對港口設施內的貨物、貨物運輸單元和貨物存放區域的詳細核查；

.2 適當時的強化核查，確保只有有單證的貨物才能進入港口設施，在那兒暫時存放並在此後裝船；

.3 車輛的強化搜查；和

.4 對封條和用於防止破壞的其他方法的更頻繁和詳細的核查。

16.36 可使用若干或全部下列方法進行貨物的詳細核查：

.1 增加對港口設施內的貨物、貨物運輸單元和貨物存放區域的核查頻度和詳細度（外觀和物理檢查）；

.2 增加使用掃瞄/探測設施、機械裝置或狗的頻度；和

.3 與發貨人或其他負責方就議定的協議和程序以外的其他強化保安措施進行協調。

3 級保安

16.37 在 3 級保安時，港口設施應遵守保安事件或其威脅的反應人員發出的指示。PFSP 應詳述港口設施在反應人員和港口設施內的船舶的密切配合下能夠採取的保安措施。它們可以包括：

.1 限制或中止港口設施全部或局部範圍內或特定船舶的貨物運動或作業；和

.2 核查港口設施內存放的危險品和有害物質的清單及其位置。

船舶物料的交付

16.38 船舶物料交付的保安措施應：

.1 確保對船舶物料和包裝完整性的核查；

.2 防止接受未經檢查的船舶物料；

.3 防止破壞；

.4 防止接受未定購的船舶物料；

.5 確保對交貨車輛的搜查；和

.6 確保在港口設施內監護交貨車輛。

16.39 對於經常使用港口設施的船舶，制定涉及該船舶、其供應商和港口設施的有關交貨通知和時間和證件的程序可能是適當的。應始終有某種辦法核實交付的物料附有它們係船舶定購者的證據。

1 級保安

16.40 在 1 級保安時，PFSP 應確定控制船舶物料交付使用的保安措施，它們可以包括：

.1 核查船舶物料；

.2 有關裝載物構成、司機詳情和車輛登記牌的預先通知；和

.3 搜查交貨車輛。

16.41 可以某些或全部下述方法進行船舶物料核查：

.1 外觀和物理檢查；和

.2 使用掃瞄/探測設備、機械裝置或狗。

2 級保安

16.42 在 2 級保安時，PFSP 應確定為強化對交付船舶物料的控制而使用的額外保安措施。它們可以包括：

.1 對船舶物料的詳細核查；

.2 對交貨車輛的詳細搜查；

.3 與船舶人員協調，在進入港口設施前根據交貨通知書核對定貨；和

.4 在港口設施內監護交貨車輛。

16.43 可使用某些或全部下列方法進行船舶物料的詳細核查：

.1 增加搜查車輛的頻度和詳細度；

.2 增加掃瞄/探測設備、機械裝置或狗的使用；和

.3 限制或禁止在規限期限內不會離開港口設施的物料進入。

3 級保安

16.44 在 3 級保安時，港口設施應遵守保安事件或其威脅的反應人員發出的指示。PFSP 應詳述港口設施在反應人員和港口設施內的船舶的密切配合下能夠採取的保安措施。它們可包括做好限制或中止在港口設施的全部或局部範圍內交付船舶物料的準備。

寄存行李的搬運

16.45 PFSP 應確定為確保寄存行李（即在檢查或搜查時不在旅客或船員身邊的任何行李，包括個人物品）在被允許進入港口設施前和，視存放安排而定，被允許在港口設施與船舶間輸送前得到識別和接受包括搜查在內的適當檢查而使用的保安措施。並非要此種行李接受港口設施和船舶兩者的檢查。在兩者都有適當設備時，檢查責任應由港口設施承擔。與船舶的密切配合是必要的，應採取步驟確保在檢查後對寄存行李作出保安的搬運。

1 級保安

16.46 在 1 級保安時，PFSP 應確定在搬運寄存行李時使用的保安措施，確保對寄存行李進行高達並包括 100%的檢查或搜查，其中可包括 X 光檢查。

2 級保安

16.47 在 2 級保安時，PFSP 應確定搬運寄存行李時使用的額外保安措施。它們應包括對所有寄存行李的 100%的 X 光檢查。

3 級保安

16.48 在 3 級保安時，港口設施應遵守保安事件或其威脅的反應人員發出的指示。PFSP 應詳述港口設施在反應人員和港口設施內的船舶的密切配合下能夠採取的保安措施。它們可以包括：

.1 對此種行李進行更廣泛的檢查，如從至少兩個不同角度對其使用 X 光；

.2 做好限制或中止搬運寄存行李的準備；和

.3 拒絕接受寄存行李進入港口設施。

監視港口設施的保安

16.49 港口設施保安組織應能在包括夜間和低能見度期間在內的所有時刻在陸上和水上監視港口設施和其附近的進港航道、港口設施內的禁區、港口設施內的船舶和船舶的周圍區域。此種監視能力可包括使用：

.1 照明；

.2 警衛，包括徒步、車輛和水上巡邏；和

.3 自動侵入探測裝置和監視設備。

16.50 使用時，自動侵入探測裝置應啓動在連續看守或監視位置上的聲響和/或視覺警報。

16.51 PFSP 應確定在每一保安級別時需要的程序和設備和確保監測設備能連續工作的方法，包括考慮到天氣或電力中斷的可能影響。

1 級保安

16.52 在 1 級保安時，PFSP 應確定要使用的保安措施；它們可以是照明、警衛或使用保安和監視設備的某種組合，使港口設施保安人員能夠：

.1 觀察整個港口設施區域，包括其岸側和水側的通道；

.2 觀察通入點、屏障和禁區；和

.3 監視使用港口設施的船舶附近區域和運動，包括增加船舶自身提供的照明。

2 級保安

16.53 在 2 級保安時，PFSP 應確定為強化監測和監視能力而使用的額外保安措施。它們可以包括：

.1 增加照明範圍和強度和監視設備，包括提供額外的照明和監視範圍；

.2 增加徒步、車輛或水上巡邏的頻度；和

.3 指派額外保安人員進行監視和巡邏。

3 級保安

16.54 在 3 級保安時，港口設施應遵守保安事件或其威脅的反應人員發出的指示。PFSP 應詳述港口設施在反應人員和港口設施中的船舶的密切配合下能夠採取的保安措施。它們可以包括：

.1 打開港口設施內的所有照明或對港口設施附近區域予以照明；

.2 打開能記錄港口設施內或其附近區域的活動的所有監視設施；和

.3 使此種監視設備的連續記錄時間最大化。

不同保安級別

16.55 PFSP 應制定在港口設施的保安級別低於對船舶使用者時港口設施能採用的程序和保安措施的細節。

本規則範圍外的活動

16.56 PFSP 應制定在下列情況下港口設施應使用的程序和保安措施的細節：

.1 它在與曾在非締約政府國家的港口內的船舶界面；

.2 它在與本規則不適用的船舶界面；和

.3 它正與固定或浮動平台或就位的移動式近海鑽井裝置界面。

保安聲明

16.57 PFSP 應確定在 PFSO 根據締約政府的指示要求“保安聲明”（DoS）或在船舶要求 DoS 時應遵守的程序。

審核、檢查和修正

16.58 PFSP 應確定 PFSO 審核 PFSP 的繼續有效性的方法和在檢查、更新或修正時 PFSP 應遵守的程序。

16.59 應按 PFSO 的決定對 PFSP 進行檢查。此外應在下列情況下對其進行檢查：

.1 港口設施的 PFSA 被更改；

.2 對 PFSP 的獨立審核或締約政府對港口設施保安組織的檢驗發現了該組織的失誤或對經認可的 PFSP 的重要內容的繼續有關提出了質疑；

.3 在發生涉及港口設施的保安事件或其威脅後；和

.4 在港口設施的所有權或經營控制權改變後。

16.60 PFSO 在對計劃作出任何檢查後可對經核准的計劃建議適當的修正案。有關下列者的 PFSP 修正案應提交核准原始 PFSP 的締約政府供審議和核准：

.1 提議的更改能根本改變保持港口設施保安所採用的方法；和

.2 撤除、改變或更換先前認為對於保持港口設施的保安為必要者的永久屏障、保安和監視設備和系統等等。

此種核准可由締約政府或其代表作出，並可帶有或不帶有對提議的更改的修正案。在核准 PFSP 時締約政府應指明哪些程序或有形改動須交由其核准。

港口設施保安計劃的核准

16.61 PFSP 必須由有關締約政府予以核准。締約政府應制定準備下列者的適當程序：

.1 向其提交 PFSP；

.2 審議 PFSP；

.3 核准 PFSP，帶有或不帶有修正案；

.4 審議在核准後提交的修正案；和

.5 檢查或審核經核准的 PFSP 的繼續有關性。

在所有階段均應採取步驟確保 PFSP 的內容始終是保密的。

港口設施符合聲明

16.62 港口設施在其領土內的締約政府可頒發適當的“港口設施符合聲明”（SoCPF），指明：

.1 該港口設施；

.2 該港口設施符合第 XI-2 章和本規則第 A 部分的規定；

.3 由締約政府規定的但不超過五年的該 SoCPF 的有效期限；和

.4 締約政府確定的此後核查安排和進行核查時的確認。

16.63 “港口設施符合聲明”應採用本規則的本部分的附錄中所載的格式。如果使用的語文不是西班牙語、法語、或英語，則該締約政府在認為適當時可包括其中一種語文的譯文。

17 港口設施保安官員

綜述

17.1 在船舶保安官員對為官方目的要上船的人員的身份證的有效性存有疑問的特別情況下，港口保安官員應予協助。

17.2 港口設施保安官員不負責對要上船人員的身份的日常核實。

此外，其他有關指導載於 15、16 和 18 節中。

18 港口設施保安培訓、操練和演習

培訓

18.1 港口設施保安官員應視情在以下某些或所有方面具有知識或接受培訓：

.1 保安管理；

.2 有關的國際公約、規則和建議書；

.3 有關的政府立法和規則；

.4 其他保安組織的責任和職能；

.5 港口設施保安評定方法；

.6 船舶和港口設施保安檢驗和檢查方法；

.7 船舶和港口的作業和狀況；

.8 船舶和港口設施保安措施；

.9 應急防備和反應以及應急規劃；

.10 保安培訓和教育的講授技術，包括保安措施和程序；

.11 處理敏感的保安信息和保安通信；

.12 對當前的保安威脅和方式的知識；

.13 對武器、危險物質和裝置的識別和探測；

.14 在無歧視的基礎上對可能威脅保安的人員的特點和行為方式的識別；

.15 逃避保安措施使用的技術；

.16 保安設施和系統及其操作局限性；

.17 進行審核、檢查、控制和監視的方法；

.18 有形搜查和非侵入檢查的方法；

.19 保安操練和演習，包括與船舶的操練和演習；和

.20 對保安操練和演習的評定。

18.2 負有具體保安職責的港口設施人員應視情在以下某些或所有方面具有知識或接受培訓：

.1 對當前的保安威脅和方式的知識；

.2 對武器、危險物質和裝置的識別和探測；

.3 對可能威脅保安的人員的特點和行為方式的識別；

.4 逃避保安措施使用的技術；

.5 人群管理和控制技術；

.6 保安通信；

.7 保安設備和系統的操作；

.8 保安設備和系統的測試、校準和保養；

.9 檢查、控制和監測技術；和

.10 人員、個人物品、行李、貨物和船舶物料的有形搜查的方法。

18.3 所有其他港口設施人員均應視情了解和熟悉港口設施保安計劃在以下某些和所有方面的有關規定：

.1 不同保安級別的意義和相應要求；

.2 對武器、危險物質和裝置的識別和探測；

.3 在無歧視的基礎上，對可能威脅保安的人員的特點和行為方式的識別；和

.4 逃避保安措施使用的技術。

操練和演習

18.4 操練和演習的目的是確保港口設施人員精通所有保安級別時的所有指定保安職責，查明需要處理的任何保安缺陷。

18.5 為確保港口保安計劃的規定得到有效實施，應至少每三個月進行一次操練，除非具體情況使其不能實行。這些操練應檢驗計劃的各個成分，如 15.11 段中列出的那些保安威脅。

18.6 各種類型的演習可包括港口保安官員和，如果有的話，締約政府的有關當局、公司保安官員或船舶保安官員的參與，應每年至少進行一次，且演習間隔不應超過 18 個月。鑑於對船舶的保安和工作影響，應要求公司保安官員和船舶保安官員參加聯合演習。這些演習應檢驗通信、協調、資源準備和反應。這些演習可以是：

.1 真實或實況的；

.2 桌面模擬或研討會；或

.3 與舉行的其他演習，如應急反應或其他的港口國當局的演習，結合在一起。

19 船舶核查和發證

無額外指導

第 B 部分的附錄

附錄 1

船舶和港口設施間的“保安聲明”的格式[2]

保安聲明

船名：	
登記港：	
IMO 編號：	
港口設施名稱：	

本“保安聲明”從.....至.....對下列活動：

.....

（列出活動和有關細節）

在下列保安級別有效

船舶的保安級別：	
港口設施的保安級別：	

本港口設施和船舶議定下列保安措施和責任以確保符合《國際船舶和港口設施保安規則》的要求。

---

[2] 本“保安聲明”的格式供在船舶和港口設施間使用。如果“保安聲明”涉及兩個船舶，則應對本範本作適當修改。

	在下欄中填寫 SSO 或 PFSO 的姓名字首表明港口設施和船舶將按有關的經核准的計劃進行活動	
活動	港口設施	船舶
確保履行所有保安職責		
監視禁區，確保只有經授權的人員才能進入		
控制對港口設施的通入		
控制對船舶的通入		
監視港口設施，包括泊區和船舶周圍區域		
監視船舶，包括泊區和船舶周圍區域		
貨物裝卸		
船舶物料交付		
搬運寄存行李		
控制人員及其個人物品的上船		
確保隨時進行船舶和港口設施間的保安通信		

本議定書的簽字證明港口設施和船舶在指明的活動期間的保安措施和安排符合第 XI-2 章和本規則第 A 部分的規定。這些規定將按其經核准的計劃業已列出的規定或議定的並在本附件中載明的具體安排實施。

日期：..... 地點：.....

下列者或其代表的簽字	
港口設施：	船舶：
（港口設施保安官員的簽字）	*（船長或船舶保安官員的簽字）*

簽字者的姓名和頭銜	
姓名	姓名
頭銜	頭銜

聯絡細節 （視情填寫） *（註明電話號碼或使用的無線電頻道或頻率）*	
港口設施：	船舶：
港口設施 港口設施保安官員	船長 船舶保安官員 公司 公司保安官員

附錄 2

港口設施“符合聲明”的格式

港口設施符合聲明

（官員鋼印） *（國家）*

聲明編號.....

由.....政府

（國家名稱）

根據《國際船舶和港口設施保安規則》(《ISPS 規則》)

第 B 部分的規定頒發

港口設施名稱：.....

港口設施地址：.....

茲證明經核查該港口設施符合第 XI-2 章和《國際船舶和港口設施保安規則》(《ISPS 規則》) 第 A 部分的規定，該港口設施按經核准的港口設施保安計劃運營。該計劃在以下方面〈注明作業類型、船型或活動或其他有關信息〉(視情刪除) 得到核准：

客船

高速客船

高速貨船

散貨船

油輪

化學品液貨船

氣體運輸船

移動式近海鑽井裝置

除上述者外的其他貨船

本“符合聲明”有效至.....，以（下頁中指明的）核查為準

頒發地點..... .....
（聲明頒發地點）
頒發日期..... .....
（經正式授權的頒證官員的簽字）

（頒證當局的鋼印或章印）

核查的簽註

*〈加入國家名稱〉*政府規定本“符合聲明”的有效性以*〈加入核查的有關細節（如強制性年度或不定期核查）〉*為準。

茲證明在按《ISPS 規則》第 B/16.62.4 款進行檢查時查明該港口設施符合本公約第 XI-2 章和《ISPS 規則》第 A 部分的有關規定。

第 1 次核查

簽字：.....
（經授權的官員的簽字）

地點：.....

日期：.....

第 2 次核查

簽字：.....
（經授權的官員的簽字）

地點：.....

日期：.....

第 3 次核查

簽字：.....
（經授權的官員的簽字）

地點：.....

日期：.....

第 4 次核查

簽字：.....
（經授權的官員的簽字）

地點：.....

日期：.....

RESOLUTION 2 OF THE CONFERENCE OF CONTRACTING GOVERNMENTS TO THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA, 1974

(adopted on 12 December 2002)

THE INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES

THE CONFERENCE,

HAVING ADOPTED amendments to the International Convention for the Safety of Life at Sea, 1974, as amended (hereinafter referred to as "the Convention"), concerning special measures to enhance maritime safety and security,

CONSIDERING that the new chapter XI-2 of the Convention makes a reference to an International Ship and Port Facility Security (ISPS) Code and requires ships, companies and port facilities to comply with the relevant requirements of part A of the International Ship and Port Facility Security (ISPS) Code, as specified in part A of the ISPS Code,

BEING OF THE OPINION that the implementation by Contracting Governments of the said chapter will greatly contribute to the enhancement of maritime safety and security and safeguarding those on board and ashore,

HAVING CONSIDERED a draft of the International Code for the Security of Ships and of Port Facilities prepared by the Maritime Safety Committee of the International Maritime Organization (hereinafter referred to as "the Organization"), at its seventy-fifth and seventy-sixth sessions, for consideration and adoption by the Conference,

1. ADOPTS the International Code for the Security of Ships and of Port Facilities (hereinafter referred to as "the Code"), the text of which is set out in the annex to the present resolution;

2. INVITES Contracting Governments to the Convention to note that the Code will take effect on 1 July 2004 upon entry into force of the new chapter XI-2 of the Convention;

3. REQUESTS the Maritime Safety Committee to keep the Code under review and amend it, as appropriate;

4. REQUESTS the Secretary-General of the Organization to transmit certified copies of the present resolution and the text of the Code contained in the annex to all Contracting Governments to the Convention;

5. FURTHER REQUESTS the Secretary-General to transmit copies of this resolution and its annex to all Members of the Organization which are not Contracting Governments to the Convention.

ANNEX

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES

PREAMBLE

1 The Diplomatic Conference on Maritime Security held in London in December 2002 adopted new provisions in the International Convention for the Safety of Life at Sea, 1974 and this Code to enhance maritime security. These new requirements form the international framework through which ships and port facilities can co-operate to detect and deter acts which threaten security in the maritime transport sector.

2 Following the tragic events of 11th September 2001, the twenty-second session of the Assembly of the International Maritime Organization ("the Organization"), in November 2001, unanimously agreed to the development of new measures relating to the security of ships and of port facilities for adoption by a Conference of Contracting Governments to the International Convention for the Safety of Life at Sea, 1974 (known as the Diplomatic Conference on Maritime Security) in December 2002. Preparation for the Diplomatic Conference was entrusted to the Organization's Maritime Safety Committee (MSC) on the basis of submissions made by Member States, intergovernmental organizations and non-governmental organizations in consultative status with the Organization.

3 The MSC, at its first extraordinary session, held also in November 2001, in order to accelerate the development and the adoption of the appropriate security measures, established an MSC Intersessional Working Group on Maritime Security. The first meeting of the MSC Intersessional Working Group on Maritime Security was held in February 2002 and the outcome of its discussions was reported to, and considered by, the seventy-fifth session of the MSC in May 2002, when an *ad hoc* Working Group was established to further develop the proposals made. The seventy-fifth session of the MSC considered the report of that Working Group and recommended that work should be taken forward through a further MSC Intersessional Working Group, which was held in September 2002. The seventy-sixth session of the MSC considered the outcome of the September 2002 session of the MSC Intersessional Working Group and the further work undertaken by the MSC Working Group held in conjunction with the Committee's seventy-sixth session in December 2002, immediately prior to the Diplomatic Conference, and agreed the final version of the proposed texts to be considered by the Diplomatic Conference.

4 The Diplomatic Conference (9 to 13 December 2002) also adopted amendments to the existing provisions of the International Convention for the Safety of Life at Sea, 1974 (SOLAS 74) accelerating the implementation of the requirement to fit Automatic Identification Systems and adopted new regulations in chapter XI-1 of SOLAS 74 covering marking of the Ship Identification Number and the carriage of a Continuous Synopsis Record. The Diplomatic Conference also adopted a number of Conference resolutions, including those covering implementation and revision of this Code, technical co-operation, and co-operative work with the International Labour Organization and World Customs Organization. It was recognized that review and amendment of certain of the new provisions regarding maritime security may be required on completion of the work of these two Organizations.

5 The provisions of chapter XI-2 of SOLAS 74 and this Code apply to ships and to port facilities. The extension of SOLAS 74 to cover port facilities was agreed on the basis that SOLAS 74 offered the speediest means of ensuring the necessary security measures entered into force and given effect quickly. However, it was further agreed that the provisions relating to port facilities should relate solely to the ship/port interface. The wider issue of the security of port areas will be the subject of further joint work between the International Maritime Organization and the International Labour Organization. It was also agreed that the provisions should not extend to the actual response to attacks or to any necessary clear-up activities after such an attack.

6 In drafting the provision, care has been taken to ensure compatibility with the provisions of the International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978, as amended, the International Safety Management (ISM) Code and the harmonized system of survey and certification.

7 The provisions represent a significant change in the approach of the international maritime industries to the issue of security in the maritime transport sector. It is recognized that they may place a significant additional burden on certain Contracting Governments. The importance of technical co-operation to assist Contracting Governments implement the provisions is fully recognized.

8 Implementation of the provisions will require continuing effective co-operation and understanding between all those involved with, or using, ships and port facilities, including ship's personnel, port personnel, passengers, cargo interests, ship and port management and those in National and Local Authorities with security responsibilities. Existing practices and procedures will have to be reviewed and changed if they do not provide an adequate level of security. In the interests of enhanced maritime security, additional responsibilities will have to be carried by the shipping and port industries and by National and Local Authorities.

9 The guidance given in part B of this Code should be taken into account when implementing the security provisions set out in chapter XI-2 of SOLAS 74 and in part A of this Code. However, it is recognized that the extent to which the guidance applies may vary depending on the nature of the port facility and of the ship, its trade and/or cargo.

10 Nothing in this Code shall 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, including the International Labour Organization Declaration of Fundamental Principles and Rights at Work as well as international standards concerning maritime and port workers.

11 Recognizing that the Convention on the Facilitation of Maritime Traffic, 1965, as amended, provides that foreign crew members shall be allowed ashore by the public authorities while the ship on which they arrive is in port, provided that the formalities on arrival of the ship have been fulfilled and the public authorities have no reason to refuse permission to come ashore for reasons of public health, public safety or public order, Contracting Governments, when approving ship and port facility security plans, should pay due cognisance to the fact that ship's personnel live and work on the vessel and need shore leave and access to shore-based seafarer welfare facilities, including medical care.

PART A

MANDATORY REQUIREMENTS REGARDING THE PROVISIONS OF CHAPTER XI-2 OF THE ANNEX TO THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA, 1974, AS AMENDED

1 GENERAL

1.1 Introduction

This part of the International Code for the Security of Ships and of Port Facilities contains mandatory provisions to which reference is made in chapter XI-2 of the International Convention for the Safety of Life at Sea, 1974, as amended.

1.2 Objectives

The objectives of this Code are:

.1 to establish an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect security threats and take preventive measures against security incidents affecting ships or port facilities used in international trade;

.2 to establish the respective roles and responsibilities of the Contracting Governments, Government agencies, local administrations and the shipping and port industries, at the national and international level, for ensuring maritime security;

.3 to ensure the early and efficient collection and exchange of security-related information;

.4 to provide a methodology for security assessments so as to have in place plans and procedures to react to changing security levels; and

.5 to ensure confidence that adequate and proportionate maritime security measures are in place.

1.3 Functional requirements

In order to achieve its objectives, this Code embodies a number of functional requirements. These include, but are not limited to:

.1 gathering and assessing information with respect to security threats and exchanging such information with appropriate Contracting Governments;

.2 requiring the maintenance of communication protocols for ships and port facilities;

.3 preventing unauthorized access to ships, port facilities and their restricted areas;

.4 preventing the introduction of unauthorized weapons, incendiary devices or explosives to ships or port facilities;

.5 providing means for raising the alarm in reaction to security threats or security incidents;

.6 requiring ship and port facility security plans based upon security assessments; and

.7 requiring training, drills and exercises to ensure familiarity with security plans and procedures.

2 **DEFINITIONS**

2.1 For the purpose of this part, unless expressly provided otherwise:

.1 *Convention* means the International Convention for the Safety of Life at Sea, 1974, as amended.

.2 *Regulation* means a regulation of the Convention.

.3 *Chapter* means a chapter of the Convention.

.4 *Ship security plan* means a plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores or the ship from the risks of a security incident.

.5 *Port facility security plan* means a plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units and ship's stores within the port facility from the risks of a security incident.

.6 *Ship security officer* means the person on board the ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan, and for liaison with the company security officer and port facility security officers.

.7 *Company security officer* means the person designated by the Company for ensuring that a ship security assessment is carried out; that a ship security plan is developed, submitted for approval, and thereafter implemented and maintained, and for liaison with port facility security officers and the ship security officer.

.8 *Port facility security officer* means the person designated as responsible for the development, implementation, revision and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

.9 *Security level 1* means the level for which minimum appropriate protective security measures shall be maintained at all times.

.10 *Security level 2* means the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a security incident.

.11 *Security level 3* means the level for which further specific protective security measures shall be maintained for a limited period of time when a security incident is probable or imminent, although it may not be possible to identify the specific target.

2.2 The term "ship", when used in this Code, includes mobile offshore drilling units and high-speed craft as defined in regulation XI-2/1.

2.3 The term "Contracting Government" in connection with any reference to a port facility, when used in sections 14 to 18, includes a reference to the Designated Authority.

2.4 Terms not otherwise defined in this part shall have the same meaning as the meaning attributed to them in chapters I and XI-2.

3 APPLICATION

3.1 This Code applies to:

.1 the following types of ships engaged on international voyages:

.1 passenger ships, including high-speed passenger craft;

.2 cargo ships, including high-speed craft, of 500 gross tonnage and upwards; and

.3 mobile offshore drilling units; and

.2 port facilities serving such ships engaged on international voyages.

3.2 Notwithstanding the provisions of section 3.1.2, Contracting Governments shall decide the extent of application of this Part of the Code to those port facilities within their territory which, although used primarily by ships not engaged on international voyages, are required, occasionally, to serve ships arriving or departing on an international voyage.

3.2.1 Contracting Governments shall base their decisions, under section 3.2, on a port facility security assessment carried out in accordance with this Part of the Code.

3.2.2 Any decision which a Contracting Government makes, under section 3.2, shall not compromise the level of security intended to be achieved by chapter XI-2 or by this Part of the Code.

3.3 This Code does not apply to warships, naval auxiliaries or other ships owned or operated by a Contracting Government and used only on Government non-commercial service.

3.4 Sections 5 to 13 and 19 of this part apply to Companies and ships as specified in regulation XI-2/4.

3.5 Sections 5 and 14 to 18 of this part apply to port facilities as specified in regulation XI-2/10.

3.6 Nothing in this Code shall prejudice the rights or obligations of States under international law.

4 RESPONSIBILITIES OF CONTRACTING GOVERNMENTS

4.1 Subject to the provisions of regulation XI-2/3 and XI-2/7, Contracting Governments shall set security levels and provide guidance for protection from security incidents. Higher security levels indicate greater likelihood of occurrence of a security incident. Factors to be considered in setting the appropriate security level include:

.1 the degree that the threat information is credible;

.2 the degree that the threat information is corroborated;

.3 the degree that the threat information is specific or imminent; and

.4 the potential consequences of such a security incident.

4.2 Contracting Governments, when they set security level 3, shall issue, as necessary, appropriate instructions and shall provide security-related information to the ships and port facilities that may be affected.

4.3 Contracting Governments may delegate to a recognized security organization certain of their security-related duties under chapter XI-2 and this Part of the Code with the exception of:

.1 setting of the applicable security level;

.2 approving a port facility security assessment and subsequent amendments to an approved assessment;

.3 determining the port facilities which will be required to designate a port facility security officer;

.4 approving a port facility security plan and subsequent amendments to an approved plan;

.5 exercising control and compliance measures pursuant to regulation XI-2/9; and

.6 establishing the requirements for a Declaration of Security.

4.4 Contracting Governments shall, to the extent they consider appropriate, test the effectiveness of the ship security plans or the port facility security plans, or of amendments to such plans, they have approved, or, in the case of ships, of plans which have been approved on their behalf.

5 DECLARATION OF SECURITY

5.1 Contracting Governments shall determine when a Declaration of Security is required by assessing the risk the ship/port interface or ship-to-ship activity poses to persons, property or the environment.

5.2 A ship can request completion of a Declaration of Security when:

.1 the ship is operating at a higher security level than the port facility or another ship it is interfacing with;

.2 there is an agreement on a Declaration of Security between Contracting Governments covering certain international voyages or specific ships on those voyages;

.3 there has been a security threat or a security incident involving the ship or involving the port facility, as applicable;

.4 the ship is at a port which is not required to have and implement an approved port facility security plan; or

.5 the ship is conducting ship-to-ship activities with another ship not required to have and implement an approved ship security plan.

5.3 Requests for the completion of a Declaration of Security, under this section, shall be acknowledged by the applicable port facility or ship.

5.4 The Declaration of Security shall be completed by:

.1 the master or the ship security officer on behalf of the ship(s); and, if appropriate,

.2 the port facility security officer or, if the Contracting Government determines otherwise, by any other body responsible for shore-side security, on behalf of the port facility.

5.5 The Declaration of Security shall address the security requirements that could be shared between a port facility and a ship (or between ships) and shall state the responsibility for each.

5.6 Contracting Governments shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by the port facilities located within their territory.

5.7 Administrations shall specify, bearing in mind the provisions of regulation XI-2/9.2.3, the minimum period for which Declarations of Security shall be kept by ships entitled to fly their flag.

6 OBLIGATIONS OF THE COMPANY

6.1 The Company shall ensure that the ship security plan contains a clear statement emphasizing the master's authority. The Company shall establish in the ship security plan that the master has the overriding authority and responsibility to make decisions with respect to the

safety and security of the ship and to request the assistance of the Company or of any Contracting Government as may be necessary.

6.2 The Company shall ensure that the company security officer, the master and the ship security officer are given the necessary support to fulfil their duties and responsibilities in accordance with chapter XI-2 and this Part of the Code.

7 SHIP SECURITY

7.1 A ship is required to act upon the security levels set by Contracting Governments as set out below.

7.2 At security level 1, the following activities shall be carried out, through appropriate measures, on all ships, taking into account the guidance given in part B of this Code, in order to identify and take preventive measures against security incidents:

.1 ensuring the performance of all ship security duties;

.2 controlling access to the ship;

.3 controlling the embarkation of persons and their effects;

.4 monitoring restricted areas to ensure that only authorized persons have access;

.5 monitoring of deck areas and areas surrounding the ship;

.6 supervising the handling of cargo and ship's stores; and

.7 ensuring that security communication is readily available.

7.3 At security level 2, additional protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of this Code.

7.4 At security level 3, further specific protective measures, specified in the ship security plan, shall be implemented for each activity detailed in section 7.2, taking into account the guidance given in part B of this Code.

7.5 Whenever security level 2 or 3 is set by the Administration, the ship shall acknowledge receipt of the instructions on change of the security level.

7.6 Prior to entering a port or whilst in a port within the territory of a Contracting Government that has set security level 2 or 3, the ship shall acknowledge receipt of this instruction and shall confirm to the port facility security officer the initiation of the implementation of the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3, in instructions issued by the Contracting Government which has set security level 3. The ship shall report any difficulties in implementation. In such cases, the port facility security officer and ship security officer shall liaise and co-ordinate the appropriate actions.

7.7 If a ship is required by the Administration to set, or is already at, a higher security level than that set for the port it intends to enter or in which it is already located, then the ship shall

advise, without delay, the competent authority of the Contracting Government within whose territory the port facility is located and the port facility security officer of the situation.

7.7.1 In such cases, the ship security officer shall liaise with the port facility security officer and co-ordinate appropriate actions, if necessary.

7.8 An Administration requiring ships entitled to fly its flag to set security level 2 or 3 in a port of another Contracting Government shall inform that Contracting Government without delay.

7.9 When Contracting Governments set security levels and ensure the provision of security-level information to ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, such ships shall be advised to maintain vigilance and report immediately to their Administration and any nearby coastal States any information that comes to their attention that might affect maritime security in the area.

7.9.1 When advising such ships of the applicable security level, a Contracting Government shall, taking into account the guidance given in part B of this Code, also advise those ships of any security measure that they should take and, if appropriate, of measures that have been taken by the Contracting Government to provide protection against the threat.

8 SHIP SECURITY ASSESSMENT

8.1 The ship security assessment is an essential and integral part of the process of developing and updating the ship security plan.

8.2 The company security officer shall ensure that the ship security assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with this section, taking into account the guidance given in part B of this Code.

8.3 Subject to the provisions of section 9.2.1, a recognized security organization may carry out the ship security assessment of a specific ship.

8.4 The ship security assessment shall include an on-scene security survey and, at least, the following elements:

.1 identification of existing security measures, procedures and operations;

.2 identification and evaluation of key shipboard operations that it is important to protect;

.3 identification of possible threats to the key shipboard operations and the likelihood of their occurrence, in order to establish and prioritize security measures; and

.4 identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

8.5 The ship security assessment shall be documented, reviewed, accepted and retained by the Company.

9 SHIP SECURITY PLAN

9.1 Each ship shall carry on board a ship security plan approved by the Administration. The plan shall make provisions for the three security levels as defined in this Part of the Code.

9.1.1 Subject to the provisions of section 9.2.1, a recognized security organization may prepare the ship security plan for a specific ship.

9.2 The Administration may entrust the review and approval of ship security plans, or of amendments to a previously approved plan, to recognized security organizations.

9.2.1 In such cases, the recognized security organization undertaking the review and approval of a ship security plan, or its amendments, for a specific ship shall not have been involved in either the preparation of the ship security assessment or of the ship security plan, or of the amendments, under review.

9.3 The submission of a ship security plan, or of amendments to a previously approved plan, for approval shall be accompanied by the security assessment on the basis of which the plan, or the amendments, has been developed.

9.4 Such a plan shall be developed, taking into account the guidance given in part B of this Code, and shall be written in the working language or languages of the ship. If the language or languages used is not English, French or Spanish, a translation into one of these languages shall be included. The plan shall address, at least, the following:

.1 measures designed to prevent weapons, dangerous substances and devices intended for use against persons, ships or ports and the carriage of which is not authorized from being taken on board the ship;

.2 identification of the restricted areas and measures for the prevention of unauthorized access to them;

.3 measures for the prevention of unauthorized access to the ship;

.4 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the ship or ship/port interface;

.5 procedures for responding to any security instructions Contracting Governments may give at security level 3;

.6 procedures for evacuation in case of security threats or breaches of security;

.7 duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects;

.8 procedures for auditing the security activities;

.9 procedures for training, drills and exercises associated with the plan;

.10 procedures for interfacing with port facility security activities;

.11 procedures for the periodic review of the plan and for updating;

.12 procedures for reporting security incidents;

.13 identification of the ship security officer;

.14 identification of the company security officer, including 24-hour contact details;

.15 procedures to ensure the inspection, testing, calibration, and maintenance of any security equipment provided on board;

.16 frequency for testing or calibration of any security equipment provided on board;

.17 identification of the locations where the ship security alert system activation points are provided; and

.18 procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting and to limit false alerts.

9.4.1 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the Company or of the ship.

9.5 The Administration shall determine which changes to an approved ship security plan or to any security equipment specified in an approved plan shall not be implemented unless the relevant amendments to the plan are approved by the Administration. Any such changes shall be at least as effective as those measures prescribed in chapter XI-2 and this Part of the Code.

9.5.1 The nature of the changes to the ship security plan or the security equipment that have been specifically approved by the Administration, pursuant to section 9.5, shall be documented in a manner that clearly indicates such approval. This approval shall be available on board and shall be presented together with the International Ship Security Certificate (or the Interim International Ship Security Certificate). If these changes are temporary, once the original approved measures or equipment are reinstated, this documentation no longer needs to be retained by the ship.

9.6 The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

9.7 The plan shall be protected from unauthorized access or disclosure.

9.8 Ship security plans are not subject to inspection by officers duly authorized by a Contracting Government to carry out control and compliance measures in accordance with regulation XI-2/9, save in circumstances specified in section 9.8.1.

9.8.1 If the officers duly authorized by a Contracting Government have clear grounds to believe that the ship is not in compliance with the requirements of chapter XI-2 or part A of this Code, and the only means to verify or rectify the non-compliance is to review the relevant requirements of the ship security plan, limited access to the specific sections of the plan relating to the non-compliance is exceptionally allowed, but only with the consent of the Contracting Government of, or the master of, the ship concerned. Nevertheless, the provisions in the plan relating to section 9.4 subsections .2, .4, .5, .7, .15, .17 and .18 of this Part of the Code are considered as

confidential information, and cannot be subject to inspection unless otherwise agreed by the Contracting Governments concerned.

10 RECORDS

10.1 Records of the following activities addressed in the ship security plan shall be kept on board for at least the minimum period specified by the Administration, bearing in mind the provisions of regulation XI-2/9.2.3:

.1 training, drills and exercises;

.2 security threats and security incidents;

.3 breaches of security;

.4 changes in security level;

.5 communications relating to the direct security of the ship such as specific threats to the ship or to port facilities the ship is, or has been, in;

.6 internal audits and reviews of security activities;

.7 periodic review of the ship security assessment;

.8 periodic review of the ship security plan;

.9 implementation of any amendments to the plan; and

.10 maintenance, calibration and testing of any security equipment provided on board, including testing of the ship security alert system.

10.2 The records shall be kept in the working language or languages of the ship. If the language or languages used are not English, French or Spanish, a translation into one of these languages shall be included.

10.3 The records may be kept in an electronic format. In such a case, they shall be protected by procedures aimed at preventing their unauthorized deletion, destruction or amendment.

10.4 The records shall be protected from unauthorized access or disclosure.

11 COMPANY SECURITY OFFICER

11.1 The Company shall designate a company security officer. A person designated as the company security officer may act as the company security officer for one or more ships, depending on the number or types of ships the Company operates, provided it is clearly identified for which ships this person is responsible. A Company may, depending on the number or types of ships they operate, designate several persons as company security officers provided it is clearly identified for which ships each person is responsible.

11.2 In addition to those specified elsewhere in this Part of the Code, the duties and responsibilities of the company security officer shall include, but are not limited to:

.1 advising the level of threats likely to be encountered by the ship, using appropriate security assessments and other relevant information;

.2 ensuring that ship security assessments are carried out;

.3 ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the ship security plan;

.4 ensuring that the ship security plan is modified, as appropriate, to correct deficiencies and satisfy the security requirements of the individual ship;

.5 arranging for internal audits and reviews of security activities;

.6 arranging for the initial and subsequent verifications of the ship by the Administration or the recognized security organization;

.7 ensuring that deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance are promptly addressed and dealt with;

.8 enhancing security awareness and vigilance;

.9 ensuring adequate training for personnel responsible for the security of the ship;

.10 ensuring effective communication and co-operation between the ship security officer and the relevant port facility security officers;

.11 ensuring consistency between security requirements and safety requirements;

.12 ensuring that, if sister-ship or fleet security plans are used, the plan for each ship reflects the ship-specific information accurately; and

.13 ensuring that any alternative or equivalent arrangements approved for a particular ship or group of ships are implemented and maintained.

12 SHIP SECURITY OFFICER

12.1 A ship security officer shall be designated on each ship.

12.2 In addition to those specified elsewhere in this Part of the Code, the duties and responsibilities of the ship security officer shall include, but are not limited to:

.1 undertaking regular security inspections of the ship to ensure that appropriate security measures are maintained;

.2 maintaining and supervising the implementation of the ship security plan, including any amendments to the plan;

.3 co-ordinating the security aspects of the handling of cargo and ship's stores with other shipboard personnel and with the relevant port facility security officers;

.4 proposing modifications to the ship security plan;

.5 reporting to the company security officer any deficiencies and non-conformities identified during internal audits, periodic reviews, security inspections and verifications of compliance and implementing any corrective actions;

.6 enhancing security awareness and vigilance on board;

.7 ensuring that adequate training has been provided to shipboard personnel, as appropriate;

.8 reporting all security incidents;

.9 co-ordinating implementation of the ship security plan with the company security officer and the relevant port facility security officer; and

.10 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any.

13 TRAINING, DRILLS AND EXERCISES ON SHIP SECURITY

13.1 The company security officer and appropriate shore-based personnel shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

13.2 The ship security officer shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

13.3 Shipboard personnel having specific security duties and responsibilities shall understand their responsibilities for ship security as described in the ship security plan and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in part B of this Code.

13.4 To ensure the effective implementation of the ship security plan, drills shall be carried out at appropriate intervals taking into account the ship type, ship personnel changes, port facilities to be visited and other relevant circumstances, taking into account the guidance given in part B of this Code.

13.5 The company security officer shall ensure the effective co-ordination and implementation of ship security plans by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

14 PORT FACILITY SECURITY

14.1 A port facility is required to act upon the security levels set by the Contracting Government within whose territory it is located. Security measures and procedures shall be applied at the port facility in such a manner as to cause a minimum of interference with, or delay to, passengers, ship, ship's personnel and visitors, goods and services.

14.2 At security level 1, the following activities shall be carried out through appropriate measures in all port facilities, taking into account the guidance given in part B of this Code, in order to identify and take preventive measures against security incidents:

.1 ensuring the performance of all port facility security duties;

.2 controlling access to the port facility;

.3 monitoring of the port facility, including anchoring and berthing area(s);

.4 monitoring restricted areas to ensure that only authorized persons have access;

.5 supervising the handling of cargo;

.6 supervising the handling of ship's stores; and

.7 ensuring that security communication is readily available.

14.3 At security level 2, additional protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in part B of this Code.

14.4 At security level 3, further specific protective measures, specified in the port facility security plan, shall be implemented for each activity detailed in section 14.2, taking into account the guidance given in part B of this Code.

14.4.1 In addition, at security level 3, port facilities are required to respond to and implement any security instructions given by the Contracting Government within whose territory the port facility is located.

14.5 When a port facility security officer is advised that a ship encounters difficulties in complying with the requirements of chapter XI-2 or this part or in implementing the appropriate measures and procedures as detailed in the ship security plan, and in the case of security level 3 following any security instructions given by the Contracting Government within whose territory the port facility is located, the port facility security officer and the ship security officer shall liaise and co-ordinate appropriate actions.

14.6 When a port facility security officer is advised that a ship is at a security level which is higher than that of the port facility, the port facility security officer shall report the matter to the competent authority and shall liaise with the ship security officer and co-ordinate appropriate actions, if necessary.

15 PORT FACILITY SECURITY ASSESSMENT

15.1 The port facility security assessment is an essential and integral part of the process of developing and updating the port facility security plan.

15.2 The port facility security assessment shall be carried out by the Contracting Government within whose territory the port facility is located. A Contracting Government may authorize a recognized security organization to carry out the port facility security assessment of a specific port facility located within its territory.

15.2.1 When the port facility security assessment has been carried out by a recognized security organization, the security assessment shall be reviewed and approved for compliance with this section by the Contracting Government within whose territory the port facility is located.

15.3 The persons carrying out the assessment shall have appropriate skills to evaluate the security of the port facility in accordance with this section, taking into account the guidance given in part B of this Code.

15.4 The port facility security assessments shall periodically be reviewed and updated, taking account of changing threats and/or minor changes in the port facility, and shall always be reviewed and updated when major changes to the port facility take place.

15.5 The port facility security assessment shall include, at least, the following elements:

.1 identification and evaluation of important assets and infrastructure it is important to protect;

.2 identification of possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures;

.3 identification, selection and prioritization of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability; and

.4 identification of weaknesses, including human factors, in the infrastructure, policies and procedures.

15.6 The Contracting Government may allow a port facility security assessment to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar. Any Contracting Government which allows such an arrangement shall communicate to the Organization particulars thereof.

15.7 Upon completion of the port facility security assessment, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of countermeasures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

16 PORT FACILITY SECURITY PLAN

16.1 A port facility security plan shall be developed and maintained, on the basis of a port facility security assessment for each port facility, adequate for the ship/port interface. The plan shall make provisions for the three security levels, as defined in this Part of the Code.

16.1.1 Subject to the provisions of section 16.2, a recognized security organization may prepare the port facility security plan of a specific port facility.

16.2 The port facility security plan shall be approved by the Contracting Government in whose territory the port facility is located.

16.3 Such a plan shall be developed taking into account the guidance given in part B of this Code and shall be in the working language of the port facility. The plan shall address, at least, the following:

.1 measures designed to prevent weapons or any other dangerous substances and devices intended for use against persons, ships or ports, and the carriage of which is not authorized, from being introduced into the port facility or on board a ship;

.2 measures designed to prevent unauthorized access to the port facility, to ships moored at the facility, and to restricted areas of the facility;

.3 procedures for responding to security threats or breaches of security, including provisions for maintaining critical operations of the port facility or ship/port interface;

.4 procedures for responding to any security instructions the Contracting Government in whose territory the port facility is located may give at security level 3;

.5 procedures for evacuation in case of security threats or breaches of security;

.6 duties of port facility personnel assigned security responsibilities and of other facility personnel on security aspects;

.7 procedures for interfacing with ship security activities;

.8 procedures for the periodic review of the plan and updating;

.9 procedures for reporting security incidents;

.10 identification of the port facility security officer, including 24-hour contact details;

.11 measures to ensure the security of the information contained in the plan;

.12 measures designed to ensure effective security of cargo and the cargo handling equipment at the port facility;

.13 procedures for auditing the port facility security plan;

.14 procedures for responding in case the ship security alert system of a ship at the port facility has been activated; and

.15 procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship, including representatives of seafarers' welfare and labour organizations.

16.4 Personnel conducting internal audits of the security activities specified in the plan or evaluating its implementation shall be independent of the activities being audited unless this is impracticable due to the size and the nature of the port facility.

16.5 The port facility security plan may be combined with, or be part of, the port security plan or any other port emergency plan or plans.

16.6 The Contracting Government in whose territory the port facility is located shall determine which changes to the port facility security plan shall not be implemented unless the relevant amendments to the plan are approved by them.

16.7 The plan may be kept in an electronic format. In such a case, it shall be protected by procedures aimed at preventing its unauthorized deletion, destruction or amendment.

16.8 The plan shall be protected from unauthorized access or disclosure.

16.9 Contracting Governments may allow a port facility security plan to cover more than one port facility if the operator, location, operation, equipment, and design of these port facilities are similar. Any Contracting Government which allows such an alternative arrangement shall communicate to the Organization particulars thereof.

17 PORT FACILITY SECURITY OFFICER

17.1 A port facility security officer shall be designated for each port facility. A person may be designated as the port facility security officer for one or more port facilities.

17.2 In addition to those specified elsewhere in this Part of the Code, the duties and responsibilities of the port facility security officer shall include, but are not limited to:

.1 conducting an initial comprehensive security survey of the port facility, taking into account the relevant port facility security assessment;

.2 ensuring the development and maintenance of the port facility security plan;

.3 implementing and exercising the port facility security plan;

.4 undertaking regular security inspections of the port facility to ensure the continuation of appropriate security measures;

.5 recommending and incorporating, as appropriate, modifications to the port facility security plan in order to correct deficiencies and to update the plan to take into account relevant changes to the port facility;

.6 enhancing security awareness and vigilance of the port facility personnel;

.7 ensuring adequate training has been provided to personnel responsible for the security of the port facility;

.8 reporting to the relevant authorities and maintaining records of occurrences which threaten the security of the port facility;

.9 co-ordinating implementation of the port facility security plan with the appropriate Company and ship security officer(s);

.10 co-ordinating with security services, as appropriate;

.11 ensuring that standards for personnel responsible for security of the port facility are met;

.12 ensuring that security equipment is properly operated, tested, calibrated and maintained, if any; and

.13 assisting ship security officers in confirming the identity of those seeking to board the ship when requested.

17.3 The port facility security officer shall be given the necessary support to fulfil the duties and responsibilities imposed by chapter XI-2 and this Part of the Code.

18 TRAINING, DRILLS AND EXERCISES ON PORT FACILITY SECURITY

18.1 The port facility security officer and appropriate port facility security personnel shall have knowledge and have received training, taking into account the guidance given in part B of this Code.

18.2 Port facility personnel having specific security duties shall understand their duties and responsibilities for port facility security, as described in the port facility security plan, and shall have sufficient knowledge and ability to perform their assigned duties, taking into account the guidance given in part B of this Code.

18.3 To ensure the effective implementation of the port facility security plan, drills shall be carried out at appropriate intervals, taking into account the types of operation of the port facility, port facility personnel changes, the type of ship the port facility is serving and other relevant circumstances, taking into account guidance given in part B of this Code.

18.4 The port facility security officer shall ensure the effective co-ordination and implementation of the port facility security plan by participating in exercises at appropriate intervals, taking into account the guidance given in part B of this Code.

19 VERIFICATION AND CERTIFICATION FOR SHIPS

19.1 Verifications

19.1.1 Each ship to which this Part of the Code applies shall be subject to the verifications specified below:

.1 an initial verification before the ship is put in service or before the certificate required under section 19.2 is issued for the first time, which shall include a complete verification of its security system and any associated security equipment covered by the relevant provisions of chapter XI-2, of this Part of the Code and of the approved ship security plan. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2 and this Part of the Code, is in satisfactory condition and fit for the service for which the ship is intended;

.2 a renewal verification at intervals specified by the Administration, but not exceeding five years, except where section 19.3 is applicable. This verification shall ensure that the security system and any associated security equipment of the ship fully complies with the applicable requirements of chapter XI-2, this Part of the Code and the approved ship security plan, is in satisfactory condition and fit for the service for which the ship is intended;

.3 at least one intermediate verification. If only one intermediate verification is carried out it shall take place between the second and third anniversary date of the certificate as defined in regulation I/2(n). The intermediate verification shall include inspection of the security system and any associated security equipment of the ship to ensure that it remains satisfactory for the service for which the ship is intended. Such intermediate verification shall be endorsed on the certificate;

.4 any additional verifications as determined by the Administration.

19.1.2 The verifications of ships shall be carried out by officers of the Administration. The Administration may, however, entrust the verifications to a recognized security organization referred to in regulation XI-2/1.

19.1.3 In every case, the Administration concerned shall fully guarantee the completeness and efficiency of the verification and shall undertake to ensure the necessary arrangements to satisfy this obligation.

19.1.4 The security system and any associated security equipment of the ship after verification shall be maintained to conform with the provisions of regulations XI-2/4.2 and XI-2/6, of this Part of the Code and of the approved ship security plan. After any verification under section 19.1.1 has been completed, no changes shall be made in the security system and in any associated security equipment or the approved ship security plan without the sanction of the Administration.

19.2 Issue or endorsement of Certificate

19.2.1 An International Ship Security Certificate shall be issued after the initial or renewal verification in accordance with the provisions of section 19.1.

19.2.2 Such Certificate shall be issued or endorsed either by the Administration or by a recognized security organization acting on behalf of the Administration.

19.2.3 Another Contracting Government may, at the request of the Administration, cause the ship to be verified and, if satisfied that the provisions of section 19.1.1 are complied with, shall issue or authorize the issue of an International Ship Security Certificate to the ship and, where appropriate, endorse or authorize the endorsement of that Certificate on the ship, in accordance with this Code.

19.2.3.1 A copy of the Certificate and a copy of the verification report shall be transmitted as soon as possible to the requesting Administration.

19.2.3.2 A Certificate so issued shall contain a statement to the effect that it has been issued at the request of the Administration and it shall have the same force and receive the same recognition as the Certificate issued under section 19.2.2.

19.2.4 The International Ship Security Certificate shall be drawn up in a form corresponding to the model given in the appendix to this Code. If the language used is not English, French or Spanish, the text shall include a translation into one of these languages.

19.3 Duration and validity of Certificate

19.3.1 An International Ship Security Certificate shall be issued for a period specified by the Administration, which shall not exceed five years.

19.3.2 When the renewal verification is completed within three months before the expiry date of the existing Certificate, the new Certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing Certificate.

19.3.2.1 When the renewal verification is completed after the expiry date of the existing Certificate, the new Certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of expiry of the existing Certificate.

19.3.2.2 When the renewal verification is completed more than three months before the expiry date of the existing Certificate, the new Certificate shall be valid from the date of completion of the renewal verification to a date not exceeding five years from the date of completion of the renewal verification.

19.3.3 If a Certificate is issued for a period of less than five years, the Administration may extend the validity of the Certificate beyond the expiry date to the maximum period specified in section 19.3.1, provided that the verifications referred to in section 19.1.1 applicable when a Certificate is issued for a period of five years are carried out as appropriate.

19.3.4 If a renewal verification has been completed and a new Certificate cannot be issued or placed on board the ship before the expiry date of the existing Certificate, the Administration or recognized security organization acting on behalf of the Administration may endorse the existing Certificate and such a Certificate shall be accepted as valid for a further period which shall not exceed five months from the expiry date.

19.3.5 If a ship, at the time when a Certificate expires, is not in a port in which it is to be verified, the Administration may extend the period of validity of the Certificate but this extension shall be granted only for the purpose of allowing the ship to complete its voyage to the port in which it is to be verified, and then only in cases where it appears proper and reasonable to do so. No Certificate shall be extended for a period longer than three months, and the ship to which an extension is granted shall not, on its arrival in the port in which it is to be verified, be entitled by virtue of such extension to leave that port without having a new Certificate. When the renewal verification is completed, the new Certificate shall be valid to a date not exceeding five years from the expiry date of the existing Certificate before the extension was granted.

19.3.6 A Certificate issued to a ship engaged on short voyages which has not been extended under the foregoing provisions of this section may be extended by the Administration for a period of grace of up to one month from the date of expiry stated on it. When the renewal verification is completed, the new Certificate shall be valid to a date not exceeding five years from the date of expiry of the existing Certificate before the extension was granted.

19.3.7 If an intermediate verification is completed before the period specified in section 19.1.1, then:

.1 the expiry date shown on the Certificate shall be amended by endorsement to a date which shall not be more than three years later than the date on which the intermediate verification was completed;

.2 the expiry date may remain unchanged provided one or more additional verifications are carried out so that the maximum intervals between the verifications prescribed by section 19.1.1 are not exceeded.

19.3.8 A Certificate issued under section 19.2 shall cease to be valid in any of the following cases:

.1 if the relevant verifications are not completed within the periods specified under section 19.1.1;

.2 if the Certificate is not endorsed in accordance with section 19.1.1.3 and 19.3.7.1, if applicable;

.3 when a Company assumes the responsibility for the operation of a ship not previously operated by that Company; and

.4 upon transfer of the ship to the flag of another State.

19.3.9 In the case of:

.1 a transfer of a ship to the flag of another Contracting Government, the Contracting Government whose flag the ship was formerly entitled to fly shall, as soon as possible, transmit to the receiving Administration copies of, or all information relating to, the International Ship Security Certificate carried by the ship before the transfer and copies of available verification reports, or

.2 a Company that assumes responsibility for the operation of a ship not previously operated by that Company, the previous Company shall, as soon as possible, transmit to the receiving Company copies of any information related to the International Ship Security Certificate or to facilitate the verifications described in section 19.4.2.

19.4 Interim certification

19.4.1 The Certificates specified in section 19.2 shall be issued only when the Administration issuing the Certificate is fully satisfied that the ship complies with the requirements of section 19.1. However, after 1 July 2004, for the purposes of:

.1 a ship without a Certificate, on delivery or prior to its entry or re-entry into service;

.2 transfer of a ship from the flag of a Contracting Government to the flag of another Contracting Government;

.3 transfer of a ship to the flag of a Contracting Government from a State which is not a Contracting Government; or

.4 a Company assuming the responsibility for the operation of a ship not previously operated by that Company

until the Certificate referred to in section 19.2 is issued, the Administration may cause an Interim International Ship Security Certificate to be issued, in a form corresponding to the model given in the appendix to this Part of the Code.

19.4.2 An Interim International Ship Security Certificate shall only be issued when the Administration or recognized security organization, on behalf of the Administration, has verified that:

.1 the ship security assessment required by this Part of the Code has been completed;

.2 a copy of the ship security plan meeting the requirements of chapter XI-2 and part A of this Code is provided on board, has been submitted for review and approval, and is being implemented on the ship;

.3 the ship is provided with a ship security alert system meeting the requirements of regulation XI-2/6, if required;

.4 the company security officer:

.1 has ensured:

.1 the review of the ship security plan for compliance with this Part of the Code;

.2 that the plan has been submitted for approval; and

.3 that the plan is being implemented on the ship; and

.2 has established the necessary arrangements, including arrangements for drills, exercises and internal audits, through which the company security officer is satisfied that the ship will successfully complete the required verification in accordance with section 19.1.1.1, within 6 months;

.5 arrangements have been made for carrying out the required verifications under section 19.1.1.1;

.6 the master, the ship security officer and other ship's personnel with specific security duties are familiar with their duties and responsibilities as specified in this Part of the Code; and with the relevant provisions of the ship security plan placed on board; and have been provided such information in the working language of the ship's personnel or languages understood by them; and

.7 the ship security officer meets the requirements of this Part of the Code.

19.4.3 An Interim International Ship Security Certificate may be issued by the Administration or by a recognized security organization authorized to act on its behalf.

19.4.4 An Interim International Ship Security Certificate shall be valid for 6 months, or until the Certificate required by section 19.2 is issued, whichever comes first, and may not be extended.

19.4.5 No Contracting Government shall cause a subsequent, consecutive Interim International Ship Security Certificate to be issued to a ship if, in the judgement of the Administration or the recognized security organization, one of the purposes of the ship or a Company in requesting such certificate is to avoid full compliance with chapter XI-2 and this Part of the Code beyond the period of the initial Interim Certificate as specified in section 19.4.4.

19.4.6 For the purposes of regulation XI-2/9, Contracting Governments may, prior to accepting an Interim International Ship Security Certificate as a valid Certificate, ensure that the requirements of sections 19.4.2.4 to 19.4.2.6 have been met.

APPENDIX TO PART A

APPENDIX 1

Form of the International Ship Security Certificate

INTERNATIONAL SHIP SECURITY CERTIFICATE

(Official seal) *(State)*

Certificate Number .....

Issued under the provisions of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES (ISPS CODE)

Under the authority of the Government of _____
(name of State)

by _____
(person(s) or organization authorized)

Name of ship :.....
Distinctive number or letters :.....
Port of registry :.....
Type of ship :.....
Gross tonnage :.....
IMO Number :.....
Name and address of the Company :.....

THIS IS TO CERTIFY:

1 that the security system and any associated security equipment of the ship has been verified in accordance with section 19.1 of part A of the ISPS Code;

2 that the verification showed that the security system and any associated security equipment of the ship is in all respects satisfactory and that the ship complies with the applicable requirements of chapter XI-2 of the Convention and part A of the ISPS Code;

3 that the ship is provided with an approved ship security plan.

Date of initial / renewal verification on which this Certificate is based .....

This Certificate is valid until .....
subject to verifications in accordance with section 19.1.1 of part A of the ISPS Code.

Issued at .....
(place of issue of the Certificate)

Date of issue ....
(signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)

ENDORSEMENT FOR INTERMEDIATE VERIFICATION

THIS IS TO CERTIFY that at an intermediate verification required by section 19.1.1 of part A of the ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Intermediate verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT FOR ADDITIONAL VERIFICATIONS*

Additional verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

Additional verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

Additional verification

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ADDITIONAL VERIFICATION IN ACCORDANCE WITH SECTION A/19.3.7.2 OF THE ISPS CODE

THIS IS TO CERTIFY that at an additional verification required by section 19.3.7.2 of part A of the ISPS Code the ship was found to comply with the relevant provisions of chapter XI-2 of the Convention and part A of the ISPS Code.

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT TO EXTEND THE CERTIFICATE IF VALID FOR LESS THAN 5 YEARS WHERE SECTION A/19.3.3 OF THE ISPS CODE APPLIES

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.3 of part A of the ISPS Code, be accepted as valid until .....

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT WHERE THE RENEWAL VERIFICATION HAS BEEN COMPLETED AND SECTION A/19.3.4 OF THE ISPS CODE APPLIES

The ship complies with the relevant provisions of part A of the ISPS Code, and the Certificate shall, in accordance with section 19.3.4 of part A of the ISPS Code, be accepted as valid until .....

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT TO EXTEND THE VALIDITY OF THE CERTIFICATE UNTIL REACHING THE PORT OF VERIFICATION WHERE SECTION A/19.3.5 OF THE ISPS CODE APPLIES OR FOR A PERIOD OF GRACE WHERE SECTION A/19.3.6 OF THE ISPS CODE APPLIES

This Certificate shall, in accordance with section 19.3.5 / 19.3.6* of part A of the ISPS Code, be accepted as valid until .....

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

ENDORSEMENT FOR ADVANCEMENT OF EXPIRY DATE WHERE SECTION A/19.3.7.1 OF THE ISPS CODE APPLIES

In accordance with section 19.3.7.1 of part A of the ISPS Code, the new expiry date** is .....

Signed .....
(Signature of authorized official)
Place .....

Date .....

(Seal or stamp of the authority, as appropriate)

---

* Delete as appropriate.

** In case of completion of this part of the Certificate, the expiry date shown on the front of the Certificate shall also be amended accordingly.

APPENDIX 2

Form of the Interim International Ship Security Certificate

INTERIM INTERNATIONAL SHIP SECURITY CERTIFICATE

(official seal) *(State)*

Certificate No. .....

Issued under the provisions of the

INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES (ISPS CODE)

Under the authority of the Government of _____
(name of State)

by _____
(person(s) or organization authorized)

Name of ship : .....
Distinctive number or letters : .....
Port of registry : .....
Type of ship : .....
Gross tonnage : .....
IMO Number : .....
Name and address of Company : .....
Is this a subsequent, consecutive Interim Certificate? Yes/ No*
If Yes, date of issue of initial Interim Certificate.....

THIS IS TO CERTIFY THAT the requirements of section A/19.4.2 of the ISPS Code have been complied with.

This Certificate is issued pursuant to section A/19.4 of the ISPS Code.

This Certificate is valid until .....

Issued at .....
(place of issue of the Certificate)

Date of issue ....
(signature of the duly authorized official issuing the Certificate)

(Seal or stamp of issuing authority, as appropriate)

* Delete as appropriate

PART B

GUIDANCE REGARDING THE PROVISIONS OF CHAPTER XI-2 OF THE ANNEX TO THE INTERNATIONAL CONVENTION FOR THE SAFETY OF LIFE AT SEA, 1974 AS AMENDED AND PART A OF THIS CODE

1 INTRODUCTION

General

1.1 The preamble of this Code indicates that chapter XI-2 and part A of this Code establish the new international framework of measures to enhance maritime security and through which ships and port facilities can co-operate to detect and deter acts which threaten security in the maritime transport sector.

1.2 This introduction outlines, in a concise manner, the processes envisaged in establishing and implementing the measures and arrangements needed to achieve and maintain compliance with the provisions of chapter XI-2 and of part A of this Code and identifies the main elements on which guidance is offered. The guidance is provided in paragraphs 2 through to 19. It also sets down essential considerations which should be taken into account when considering the application of the guidance relating to ships and port facilities.

1.3 If the reader's interest relates to ships alone, it is strongly recommended that this Part of the Code is still read as a whole, particularly the paragraphs relating to port facilities. The same applies to those whose primary interest is port facilities; they should also read the paragraphs relating to ships.

1.4 The guidance provided in the following paragraphs relates primarily to protection of the ship when it is at a port facility. There could, however, be situations when a ship may pose a threat to the port facility, e.g. because, once within the port facility, it could be used as a base from which to launch an attack. When considering the appropriate security measures to respond to ship-based security threats, those completing the port facility security assessment or preparing the port facility security plan should consider making appropriate adaptations to the guidance offered in the following paragraphs.

1.5 The reader is advised that nothing in this Part of the Code should be read or interpreted in conflict with any of the provisions of either chapter XI-2 or part A of this Code and that the aforesaid provisions always prevail and override any unintended inconsistency which may have been inadvertently expressed in this Part of the Code. The guidance provided in this Part of the Code should always be read, interpreted and applied in a manner which is consistent with the aims, objectives and principles established in chapter XI-2 and part A of this Code.

Responsibilities of Contracting Governments

1.6 Contracting Governments have, under the provisions of chapter XI-2 and part A of this Code, various responsibilities, which, amongst others, include:

- setting the applicable security level;

- approving the ship security plan (SSP) and relevant amendments to a previously approved plan;

- verifying the compliance of ships with the provisions of chapter XI-2 and part A of this Code and issuing to ships the International Ship Security Certificate;

- determining which of the port facilities located within their territory are required to designate a port facility security officer (PFSO) who will be responsible for the preparation of the port facility security plan;

- ensuring completion and approval of the port facility security assessment (PFSA) and of any subsequent amendments to a previously approved assessment;

- approving the port facility security plan (PFSP) and any subsequent amendments to a previously approved plan;

- exercising control and compliance measures;

- testing approved plans; and

- communicating information to the International Maritime Organization and to the shipping and port industries.

1.7 Contracting Governments can designate, or establish, Designated Authorities within Government to undertake, with respect to port facilities, their security duties under chapter XI-2 and part A of this Code and allow recognized security organizations to carry out certain work with respect to port facilities, but the final decision on the acceptance and approval of this work should be given by the Contracting Government or the Designated Authority. Administrations may also delegate the undertaking of certain security duties, relating to ships, to recognized security organizations. The following duties or activities cannot be delegated to a recognized security organization:

- setting of the applicable security level;

- determining which of the port facilities located within the territory of a Contracting Government are required to designate a PFSO and to prepare a PFSP;

- approving a PFSA or any subsequent amendments to a previously approved assessment;

- approving a PFSP or any subsequent amendments to a previously approved plan;

- exercising control and compliance measures; and

- establishing the requirements for a Declaration of Security.

Setting the security level

1.8 The setting of the security level applying at any particular time is the responsibility of Contracting Governments and can apply to ships and port facilities. Part A of this Code defines three security levels for international use. These are:

- Security level 1, normal; the level at which ships and port facilities normally operate;

- Security level 2, heightened; the level applying for as long as there is a heightened risk of a security incident; and

- Security level 3, exceptional; the level applying for the period of time when there is the probable or imminent risk of a security incident.

The Company and the ship

1.9 Any Company operating ships to which chapter XI-2 and part A of this Code apply has to designate a CSO for the Company and a SSO for each of its ships. The duties, responsibilities and training requirements of these officers and requirements for drills and exercises are defined in part A of this Code.

1.10 The company security officer's responsibilities include, in brief amongst others, ensuring that a ship security assessment (SSA) is properly carried out, that a SSP is prepared and submitted for approval by, or on behalf of, the Administration and thereafter is placed on board each ship to which part A of this Code applies and in respect of which that person has been appointed as the CSO.

1.11 The SSP should indicate the operational and physical security measures the ship itself should take to ensure it always operates at security level 1. The plan should also indicate the additional, or intensified, security measures the ship itself can take to move to and operate at security level 2 when instructed to do so. Furthermore, the plan should indicate the possible preparatory actions the ship could take to allow prompt response to the instructions that may be issued to the ship by those responding at security level 3 to a security incident or threat thereof.

1.12 The ships to which the requirements of chapter XI-2 and part A of this Code apply are required to have, and operated in accordance with, a SSP approved by, or on behalf of, the Administration. The CSO and the SSO should monitor the continuing relevance and effectiveness of the plan, including the undertaking of internal audits. Amendments to any of the elements of an approved plan, for which the Administration has determined that approval is required, have to be submitted for review and approval before their incorporation into the approved plan and their implementation by the ship.

1.13 The ship has to carry an International Ship Security Certificate indicating that it complies with the requirements of chapter XI-2 and part A of this Code. Part A of this Code includes provisions relating to the verification and certification of the ship's compliance with the requirements on an initial, renewal and intermediate verification basis.

1.14 When a ship is at a port or is proceeding to a port of a Contracting Government, the Contracting Government has the right, under the provisions of regulation XI-2/9, to exercise various control and compliance measures with respect to that ship. The ship is subject to port State control inspections but such inspections will not normally extend to examination of the SSP itself except in specific circumstances. The ship may also be subject to additional control measures if the Contracting Government exercising the control and compliance measures has reason to believe that the security of the ship has, or the port facilities it has served have, been compromised.

1.15 The ship is also required to have on board information, to be made available to Contracting Governments upon request, indicating who is responsible for deciding the employment of the ship's personnel and for deciding various aspects relating to the employment of the ship.

The port facility

1.16 Each Contracting Government has to ensure completion of a PFSA for each of the port facilities, located within its territory, serving ships engaged on international voyages. The Contracting Government, a Designated Authority or a recognized security organization may carry out this assessment. The completed PFSA has to be approved by the Contracting Government or the Designated Authority concerned. This approval cannot be delegated. Port facility security assessments should be periodically reviewed.

1.17 The PFSA is fundamentally a risk analysis of all aspects of a port facility's operation in order to determine which part(s) of it are more susceptible, and/or more likely, to be the subject of attack. Security risk is a function of the threat of an attack coupled with the vulnerability of the target and the consequences of an attack.

The assessment must include the following components:

- determination of the perceived threat to port installations and infrastructure;
- identification of the potential vulnerabilities; and
- calculation of the consequences of incidents.

On completion of the analysis, it will be possible to produce an overall assessment of the level of risk. The PFSA will help determine which port facilities are required to appoint a PFSO and prepare a PFSP.

1.18 The port facilities which have to comply with the requirements of chapter XI-2 and part A of this Code are required to designate a PFSO. The duties, responsibilities and training requirements of these officers and requirements for drills and exercises are defined in part A of this Code.

1.19 The PFSP should indicate the operational and physical security measures the port facility should take to ensure that it always operates at security level 1. The plan should also indicate the additional, or intensified, security measures the port facility can take to move to and operate at security level 2 when instructed to do so. Furthermore, the plan should indicate the possible preparatory actions the port facility could take to allow prompt response to the instructions that may be issued by those responding at security level 3 to a security incident or threat thereof.

1.20 The port facilities which have to comply with the requirements of chapter XI-2 and part A of this Code are required to have, and operate in accordance with, a PFSP approved by the Contracting Government or by the Designated Authority concerned. The PFSO should implement its provisions and monitor the continuing effectiveness and relevance of the plan, including commissioning internal audits of the application of the plan. Amendments to any of the elements of an approved plan, for which the Contracting Government or the Designated Authority concerned has determined that approval is required, have to be submitted for review and approval before their incorporation into the approved plan and their implementation at the port facility. The Contracting Government or the Designated Authority concerned may test the

effectiveness of the plan. The PFSA covering the port facility or on which the development of the plan has been based should be regularly reviewed. All these activities may lead to amendment of the approved plan. Any amendments to specified elements of an approved plan will have to be submitted for approval by the Contracting Government or by the Designated Authority concerned.

1.21 Ships using port facilities may be subject to the port State control inspections and additional control measures outlined in regulation XI-2/9. The relevant authorities may request the provision of information regarding the ship, its cargo, passengers and ship's personnel prior to the ship's entry into port. There may be circumstances in which entry into port could be denied.

Information and communication

1.22 Chapter XI-2 and part A of this Code require Contracting Governments to provide certain information to the International Maritime Organization and for information to be made available to allow effective communication between Contracting Governments and between company security officers/ship security officers and the port facility security officers.

2 DEFINITIONS

2.1 No guidance is provided with respect to the definitions set out in chapter XI-2 or part A of this Code.

2.2 For the purpose of this Part of the Code:

.1 "section" means a section of part A of the Code and is indicated as "*section A/<followed by the number of the section>*";

.2 "paragraph" means a paragraph of this Part of the Code and is indicated as "*paragraph <followed by the number of the paragraph>*"; and

.3 "Contracting Government", when used in paragraphs 14 to 18, means the "Contracting Government within whose territory the port facility is located" and includes a reference to the Designated Authority.

3 APPLICATION

General

3.1 The guidance given in this Part of the Code should be taken into account when implementing the requirements of chapter XI-2 and part A of this Code.

3.2 However, it should be recognized that the extent to which the guidance on ships applies will depend on the type of ship, its cargoes and/or passengers, its trading pattern and the characteristics of the port facilities visited by the ship.

3.3 Similarly, in relation to the guidance on port facilities, the extent to which this guidance applies will depend on the port facilities, the types of ships using the port facility, the types of cargo and/or passengers and the trading patterns of visiting ships.

3.4 The provisions of chapter XI-2 and part A of this Code are not intended to apply to port facilities designed and used primarily for military purposes.

4 RESPONSIBILITIES OF CONTRACTING GOVERNMENTS

Security of assessments and plans

4.1 Contracting Governments should ensure that appropriate measures are in place to avoid unauthorized disclosure of, or access to, security-sensitive material relating to ship security assessments (SSAs), ship security plans (SSPs), port facility security assessments (PFSAs) and port facility security plans (PFSPs) , and to individual assessments or plans.

Designated Authorities

4.2 Contracting Governments may identify a Designated Authority within Government to undertake their security duties relating to port facilities as set out in chapter XI-2 or part A of this Code.

Recognized security organizations

4.3 Contracting Governments may authorize a recognized security organization (RSO) to undertake certain security-related activities, including:

.1 approval of ship security plans, or amendments thereto, on behalf of the Administration;

.2 verification and certification of compliance of ships with the requirements of chapter XI-2 and part A of this Code on behalf of the Administration; and

.3 conducting port facility security assessments required by the Contracting Government.

4.4 An RSO may also advise or provide assistance to Companies or port facilities on security matters, including ship security assessments, ship security plans, port facility security assessments and port facility security plans. This can include completion of a SSA or SSP or PFSA or PFSP. If an RSO has done so in respect of a SSA or SSP, that RSO should not be authorized to approve that SSP.

4.5 When authorizing an RSO, Contracting Governments should give consideration to the competency of such an organization. An RSO should be able to demonstrate:

.1 expertise in relevant aspects of security;

.2 appropriate knowledge of ship and port operations, including knowledge of ship design and construction if providing services in respect of ships and of port design and construction if providing services in respect of port facilities;

.3 their capability to assess the likely security risks that could occur during ship and port facility operations, including the ship/port interface, and how to minimize such risks;

.4 their ability to maintain and improve the expertise of their personnel;

.5 their ability to monitor the continuing trustworthiness of their personnel;

.6 their ability to maintain appropriate measures to avoid unauthorized disclosure of, or access to, security-sensitive material;

.7 their knowledge of the requirements of chapter XI-2 and part A of this Code and relevant national and international legislation and security requirements;

.8 their knowledge of current security threats and patterns;

.9 their knowledge of recognition and detection of weapons, dangerous substances and devices;

.10 their knowledge of recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.11 their knowledge of techniques used to circumvent security measures; and

.12 their knowledge of security and surveillance equipment and systems and their operational limitations.

When delegating specific duties to a RSO, Contracting Governments, including Administrations, should ensure that the RSO has the competencies needed to undertake the task.

4.6 A recognized organization, as referred to in regulation I/6 and fulfilling the requirements of regulation XI-1/1, may be appointed as a RSO provided it has the appropriate security-related expertise listed in paragraph 4.5.

4.7 A port or harbour Authority or port facility operator may be appointed as a RSO provided it has the appropriate security-related expertise listed in paragraph 4.5.

Setting the security level

4.8 In setting the security level, Contracting Governments should take account of general and specific threat information. Contracting Governments should set the security level applying to ships or port facilities at one of three levels:

- Security level 1, normal; the level at which the ship or port facility normally operates;

- Security level 2, heightened; the level applying for as long as there is a heightened risk of a security incident; and

- Security level 3, exceptional; the level applying for the period of time when there is the probable or imminent risk of a security incident.

4.9 Setting security level 3 should be an exceptional measure applying only when there is credible information that a security incident is probable or imminent. Security level 3 should only be set for the duration of the identified security threat or actual security incident. While the security levels may change from security level 1, through security level 2 to security level 3, it is also possible that the security levels will change directly from security level 1 to security level 3.

4.10 At all times the master of a ship has the ultimate responsibility for the safety and security of the ship. Even at security level 3 a master may seek clarification or amendment of instructions issued by those responding to a security incident, or threat thereof, if there are reasons to believe that compliance with any instruction may imperil the safety of the ship.

4.11 The CSO or the SSO should liaise at the earliest opportunity with the PFSO of the port facility the ship is intended to visit to establish the security level applying for that ship at the port facility. Having established contact with a ship, the PFSO should advise the ship of any subsequent change in the port facility's security level and should provide the ship with any relevant security information.

4.12 While there may be circumstances when an individual ship may be operating at a higher security level than the port facility it is visiting, there will be no circumstances when a ship can have a lower security level than the port facility it is visiting. If a ship has a higher security level than the port facility it intends to use, the CSO or SSO should advise the PFSO without delay. The PFSO should undertake an assessment of the particular situation in consultation with the CSO or SSO and agree on appropriate security measures with the ship, which may include completion and signing of a Declaration of Security.

4.13 Contracting Governments should consider how information on changes in security levels should be promulgated rapidly. Administrations may wish to use NAVTEX messages or Notices to Mariners as the method for notifying such changes in security levels to the ship and to CSO and SSO. Or, they may wish to consider other methods of communication that provide equivalent or better speed and coverage. Contracting Governments should establish means of notifying PFSOs of changes in security levels. Contracting Governments should compile and maintain the contact details for a list of those who need to be informed of changes in security levels. Whereas the security level need not be regarded as being particularly sensitive, the underlying threat information may be highly sensitive. Contracting Governments should give careful consideration to the type and detail of the information conveyed and the method by which it is conveyed to SSOs, CSOs and PFSOs.

Contact points and information on port facility security plans

4.14 Where a port facility has a PFSP, that fact has to be communicated to the Organization and that information must also be made available to CSOs and SSOs. No further details of the PFSP have to be published other than that it is in place. Contracting Governments should consider establishing either central or regional points of contact, or other means of providing up-to-date information on the locations where PFSPs are in place, together with contact details for the relevant PFSO. The existence of such contact points should be publicized. They could also provide information on the recognized security organizations appointed to act on behalf of the Contracting Government, together with details of the specific responsibility and conditions of authority delegated to such recognized security organizations.

4.15 In the case of a port that does not have a PFSP (and therefore does not have a PFSO), the central or regional point of contact should be able to identify a suitably qualified person ashore who can arrange for appropriate security measures to be in place, if needed, for the duration of the ship's visit.

4.16 Contracting Governments should also provide the contact details of Government officers to whom an SSO, a CSO and a PFSO can report security concerns. These Government officers should assess such reports before taking appropriate action. Such reported concerns may have a bearing on the security measures falling under the jurisdiction of another Contracting

Government. In that case, the Contracting Governments should consider contacting their counterpart in the other Contracting Government to discuss whether remedial action is appropriate. For this purpose, the contact details of the Government officers should be communicated to the International Maritime Organization.

4.17 Contracting Governments should also make the information indicated in paragraphs 4.14 to 4.16 available to other Contracting Governments on request.

Identification documents

4.18 Contracting Governments are encouraged to issue appropriate identification documents to Government officials entitled to board ships or enter port facilities when performing their official duties and to establish procedures whereby the authenticity of such documents might be verified.

Fixed and floating platforms and mobile offshore drilling units on location

4.19 Contracting Governments should consider establishing appropriate security measures for fixed and floating platforms and mobile offshore drilling units on location to allow interaction with ships which are required to comply with the provisions of chapter XI-2 and part A of this Code.

Ships which are not required to comply with part A of this Code

4.20 Contracting Governments should consider establishing appropriate security measures to enhance the security of ships to which chapter XI-2 and part A of this Code do not apply and to ensure that any security provisions applying to such ships allow interaction with ships to which part A of this Code applies.

Threats to ships and other incidents at sea

4.21 Contracting Governments should provide general guidance on the measures considered appropriate to reduce the security risk to ships flying their flag when at sea. They should provide specific advice on the action to be taken in accordance with security levels 1 to 3, if:

.1 there is a change in the security level applying to the ship while it is at sea, e.g. because of the geographical area in which it is operating or relating to the ship itself; and

.2 there is a security incident or threat thereof involving the ship while at sea.

Contracting Governments should establish the best methods and procedures for these purposes. In the case of an imminent attack, the ship should seek to establish direct communication with those responsible in the flag State for responding to security incidents.

4.22 Contracting Governments should also establish a point of contact for advice on security for any ship:

.1 entitled to fly their flag; or

.2 operating in their territorial sea or having communicated an intention to enter their territorial sea.

4.23 Contracting Governments should offer advice to ships operating in their territorial sea or having communicated an intention to enter their territorial sea, which could include advice:

.1 to alter or delay their intended passage;

.2 to navigate on a particular course or proceed to a specific location;

.3 on the availability of any personnel or equipment that could be placed on the ship;

.4 to co-ordinate the passage, arrival into port or departure from port, to allow escort by patrol craft or aircraft (fixed-wing or helicopter).

Contracting Governments should remind ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, of any temporary restricted areas that they have published.

4.24 Contracting Governments should recommend that ships operating in their territorial sea, or having communicated an intention to enter their territorial sea, implement expeditiously, for the ship's protection and for the protection of other ships in the vicinity, any security measure the Contracting Government may have advised.

4.25 The plans prepared by the Contracting Governments for the purposes given in paragraph 4.22 should include information on an appropriate point of contact, available on a 24-hour basis, within the Contracting Government including the Administration. These plans should also include information on the circumstances in which the Administration considers assistance should be sought from nearby coastal States, and a procedure for liaison between PFSOs and SSOs.

Alternative security agreements

4.26 Contracting Governments, in considering how to implement chapter XI-2 and part A of this Code, may conclude one or more agreements with one or more Contracting Governments. The scope of an agreement is limited to short international voyages on fixed routes between port facilities in the territory of the parties to the agreement. When concluding an agreement, and thereafter, the Contracting Governments should consult other Contracting Governments and Administrations with an interest in the effects of the agreement. Ships flying the flag of a State that is not party to the agreement should only be allowed to operate on the fixed routes covered by the agreement if their Administration agrees that the ship should comply with the provisions of the agreement and requires the ship to do so. In no case can such an agreement compromise the level of security of other ships and port facilities not covered by it, and specifically, all ships covered by such an agreement may not conduct ship-to-ship activities with ships not so covered. Any operational interface undertaken by ships covered by the agreement should be covered by it. The operation of each agreement must be continually monitored and amended when the need arises and in any event should be reviewed every 5 years.

Equivalent arrangements for port facilities

4.27 For certain specific port facilities with limited or special operations but with more than occasional traffic, it may be appropriate to ensure compliance by security measures equivalent to those prescribed in chapter XI-2 and in part A of this Code. This can, in particular, be the case for terminals such as those attached to factories, or quaysides with no frequent operations.

Manning level

4.28 In establishing the minimum safe manning of a ship, the Administration should take into account that the minimum safe manning provisions established by regulation V/14 only address the safe navigation of the ship. The Administration should also take into account any additional workload which may result from the implementation of the SSP and ensure that the ship is sufficiently and effectively manned. In doing so, the Administration should verify that ships are able to implement the hours of rest and other measures to address fatigue which have been promulgated by national law, in the context of all shipboard duties assigned to the various shipboard personnel.

Control and compliance measures

General

4.29 Regulation XI-2/9 describes the control and compliance measures applicable to ships under chapter XI-2. It is divided into three distinct sections; control of ships already in a port, control of ships intending to enter a port of another Contracting Government, and additional provisions applicable to both situations.

4.30 Regulation XI-2/9.1, Control of ships in port, implements a system for the control of ships while in the port of a foreign country where duly authorized officers of the Contracting Government ("duly authorized officers") have the right to go on board the ship to verify that the required certificates are in proper order. Then, if there are clear grounds to believe the ship does not comply, control measures such as additional inspections or detention may be taken. This reflects current control systems. Regulation XI-2/9.1 builds on such systems and allows for additional measures (including expulsion of a ship from a port to be taken as a control measure) when duly authorized officers have clear grounds for believing that a ship is in non-compliance with the requirements of chapter XI-2 or part A of this Code. Regulation XI-2/9.3 describes the safeguards that promote fair and proportionate implementation of these additional measures.

4.31 Regulation XI-2/9.2 applies control measures to ensure compliance to ships intending to enter a port of another Contracting Government and introduces an entirely different concept of control within chapter XI-2, applying to security only. Under this regulation, measures may be implemented prior to the ship entering port, to better ensure security. Just as in regulation XI-2/9.1, this additional control system is based on the concept of clear grounds for believing the ship does not comply with chapter XI-2 or part A of this Code, and includes significant safeguards in regulations XI-2/9.2.2 and XI-2/9.2.5 as well as in regulation XI-2/9.3.

4.32 Clear grounds that the ship is not in compliance means evidence or reliable information that the ship does not correspond with the requirements of chapter XI-2 or part A of this Code, taking into account the guidance given in this Part of the Code. Such evidence or reliable information may arise from the duly authorized officer's professional judgement or observations gained while verifying the ship's International Ship Security Certificate or Interim International Ship Security Certificate issued in accordance with part A of this Code ("Certificate") or from other sources. Even if a valid Certificate is on board the ship, the duly authorized officers may still have clear grounds for believing that the ship is not in compliance based on their professional judgement.

4.33 Examples of possible clear grounds under regulations XI-2/9.1 and XI-2/9.2 may include, when relevant:

.1 evidence from a review of the certificate that it is not valid or it has expired;

.2 evidence or reliable information that serious deficiencies exist in the security equipment, documentation or arrangements required by chapter XI-2 and part A of this Code;

.3 receipt of a report or complaint which, in the professional judgement of the duly authorized officer, contains reliable information clearly indicating that the ship does not comply with the requirements of chapter XI-2 or part A of this Code;

.4 evidence or observation gained by a duly authorized officer using professional judgement that the master or ship's personnel is not familiar with essential shipboard security procedures or cannot carry out drills related to the security of the ship or that such procedures or drills have not been carried out;

.5 evidence or observation gained by a duly authorized officer using professional judgement that key members of ship's personnel are not able to establish proper communication with any other key members of ship's personnel with security responsibilities on board the ship;

.6 evidence or reliable information that the ship has embarked persons or loaded stores or goods at a port facility or from another ship where either the port facility or the other ship is in violation of chapter XI-2 or part A of this Code, and the ship in question has not completed a Declaration of Security, nor taken appropriate, special or additional security measures or has not maintained appropriate ship security procedures;

.7 evidence or reliable information that the ship has embarked persons or loaded stores or goods at a port facility or from another source (e.g., another ship or helicopter transfer) where either the port facility or the other source is not required to comply with chapter XI-2 or part A of this Code, and the ship has not taken appropriate, special or additional security measures or has not maintained appropriate security procedures; and

.8 the ship holding a subsequent, consecutively issued Interim International Ship Security Certificate as described in section A/19.4, and, in the professional judgement of an officer duly authorized, one of the purposes of the ship or a Company in requesting such a Certificate is to avoid full compliance with chapter XI-2 and part A of this Code beyond the period of the initial Interim Certificate as described in section A/19.4.4.

4.34 The international law implications of regulation XI-2/9 are particularly relevant, and the regulation should be implemented with regulation XI-2/2.4 in mind, as the potential exists for situations where either measures will be taken which fall outside the scope of chapter XI-2, or where rights of affected ships, outside chapter XI-2, should be considered. Thus, regulation XI-2/9 does not prejudice the Contracting Government from taking measures having a basis in, and consistent with, international law to ensure the safety or security of persons, ships, port facilities and other property in cases where the ship, although in compliance with chapter XI-2 and part A of this Code, is still considered to present a security risk.

4.35 When a Contracting Government imposes control measures on a ship, the Administration should, without delay, be contacted with sufficient information to enable the Administration to fully liaise with the Contracting Government.

Control of ships in port

4.36 Where the non-compliance is either a defective item of equipment or faulty documentation leading to the ship's detention and the non-compliance cannot be remedied in the port of inspection, the Contracting Government may allow the ship to sail to another port provided that any conditions agreed between the port States and the Administration or master are met.

Ships intending to enter the port of another Contracting Government

4.37 Regulation XI-2/9.2.1 lists the information Contracting Governments may require from a ship as a condition of entry into port. One item of information listed is confirmation of any special or additional measures taken by the ship during its last 10 calls at a port facility. Examples could include:

.1 records of the measures taken while visiting a port facility located in the territory of a State which is not a Contracting Government, especially those measures that would normally have been provided by port facilities located in the territories of Contracting Governments; and

.2 any Declarations of Security that were entered into with port facilities or other ships.

4.38 Another item of information listed, that may be required as a condition of entry into port, is confirmation that appropriate ship security procedures were maintained during ship-to-ship activity conducted within the period of the last 10 calls at a port facility. It would not normally be required to include records of transfers of pilots or of customs, immigration or security officials nor bunkering, lightering, loading of supplies and unloading of waste by ship within port facilities as these would normally fall within the auspices of the PFSP. Examples of information that might be given include:

.1 records of the measures taken while engaged in a ship-to-ship activity with a ship flying the flag of a State which is not a Contracting Government, especially those measures that would normally have been provided by ships flying the flag of Contracting Governments;

.2 records of the measures taken while engaged in a ship-to-ship activity with a ship that is flying the flag of a Contracting Government but is not required to comply with the provisions of chapter XI-2 and part A of this Code, such as a copy of any security certificate issued to that ship under other provisions; and

.3 in the event that persons or goods rescued at sea are on board, all known information about such persons or goods, including their identities when known and the results of any checks run on behalf of the ship to establish the security status of those rescued. It is not the intention of chapter XI-2 or part A of this Code to delay or prevent the delivery of those in distress at sea to a place of safety. It is the sole intention of chapter XI-2 and part A of this Code to provide States with enough appropriate information to maintain their security integrity.

4.39 Examples of other practical security-related information that may be required as a condition of entry into port in order to assist with ensuring the safety and security of persons, port facilities, ships and other property include:

.1 information contained in the Continuous Synopsis Record;

.2 location of the ship at the time the report is made;

.3 expected time of arrival of the ship in port;

.4 crew list;

.5 general description of cargo aboard the ship;

.6 passenger list; and

.7 information required to be carried under regulation XI-2/5.

4.40 Regulation XI-2/9.2.5 allows the master of a ship, upon being informed that the coastal or port State will implement control measures under regulation XI-2/9.2, to withdraw the intention for the ship to enter port. If the master withdraws that intention, regulation XI-2/9 no longer applies, and any other steps that are taken must be based on, and consistent with, international law.

Additional provisions

4.41 In all cases where a ship is denied entry or is expelled from a port, all known facts should be communicated to the authorities of relevant States. This communication should consist of the following, when known:

.1 name of ship, its flag, the Ship Identification Number, call sign, ship type and cargo;

.2 reason for denying entry or for expulsion from port or port areas;

.3 if relevant, the nature of any security non-compliance;

.4 if relevant, details of any attempts made to rectify any non-compliance, including any conditions imposed on the ship for the voyage;

.5 past port(s) of call and next declared port of call;

.6 time of departure and likely estimated time of arrival at those ports;

.7 any instructions given to the ship, e.g., reporting on its route;

.8 available information on the security level at which the ship is currently operating;

.9 information regarding any communications the port State has had with the Administration;

.10 contact point within the port State making the report for the purpose of obtaining further information;

.11 crew list; and

.12 any other relevant information.

4.42 Relevant States to contact should include those along the ship's intended passage to its next port, particularly if the ship intends to enter the territorial sea of that coastal State. Other relevant States could include previous ports of call, so that further information might be obtained and security issues relating to the previous ports resolved.

4.43 In exercising control and compliance measures, the duly authorized officers should ensure that any measures or steps imposed are proportionate. Such measures or steps should be reasonable and of the minimum severity and duration necessary to rectify or mitigate the non-compliance.

4.44 The word "delay" in regulation XI-2/9.3.5.1 also refers to situations where, pursuant to actions taken under this regulation, the ship is unduly denied entry into port or the ship is unduly expelled from port.

Non-Party ships and ships below Convention size

4.45 With respect to ships flying the flag of a State which is not a Contracting Government to the Convention and not a Party to the 1988 SOLAS Protocol[1], Contracting Governments should not give more favourable treatment to such ships. Accordingly, the requirements of regulation XI-2/9 and the guidance provided in this Part of the Code should be applied to those ships.

4.46 Ships below Convention size are subject to measures by which States maintain security. Such measures should be taken with due regard to the requirements in chapter XI-2 and the guidance provided in this Part of the Code.

5 DECLARATION OF SECURITY

General

5.1 A Declaration of Security (DoS) should be completed when the Contracting Government of the port facility deems it to be necessary or when a ship deems it necessary.

5.1.1 The need for a DoS may be indicated by the results of the port facility security assessment (PFSA) and the reasons and circumstances in which a DoS is required should be set out in the port facility security plan (PFSP).

5.1.2 The need for a DoS may be indicated by an Administration for ships entitled to fly its flag or as a result of a ship security assessment (SSA) and should be set out in the ship security plan (SSP).

5.2 It is likely that a DoS will be requested at higher security levels, when a ship has a higher security level than the port facility, or another ship with which it interfaces, and for ship/port

[1] Protocol of 1988 relating to the International Convention for the Safety of Life at Sea, 1974.

interface or ship-to-ship activities that pose a higher risk to persons, property or the environment for reasons specific to that ship, including its cargo or passengers or the circumstances at the port facility or a combination of these factors.

5.2.1 In the case that a ship or an Administration, on behalf of ships entitled to fly its flag, requests completion of a DoS, the port facility security officer (PFSO) or ship security officer (SSO) should acknowledge the request and discuss appropriate security measures.

5.3 A PFSO may also initiate a DoS prior to ship/port interfaces that are identified in the approved PFSA as being of particular concern. Examples may include embarking or disembarking passengers and the transfer, loading or unloading of dangerous goods or hazardous substances. The PFSA may also identify facilities at or near highly populated areas or economically significant operations that warrant a DoS.

5.4 The main purpose of a DoS is to ensure agreement is reached between the ship and the port facility or with other ships with which it interfaces as to the respective security measures each will undertake in accordance with the provisions of their respective approved security plans.

5.4.1 The agreed DoS should be signed and dated by both the port facility and the ship(s), as applicable, to indicate compliance with chapter XI-2 and part A of this Code and should include its duration, the relevant security level or levels and the relevant contact details.

5.4.2 A change in the security level may require that a new or revised DoS be completed.

5.5 The DoS should be completed in English, French or Spanish or in a language common to both the port facility and the ship or the ships, as applicable.

5.6 A model DoS is included in appendix 1 to this Part of the Code. This model is for a DoS between a ship and a port facility. If the DoS is to cover two ships this model should be appropriately adjusted.

6 OBLIGATIONS OF THE COMPANY

General

6.1 Regulation XI-2/5 requires the Company to provide the master of the ship with information to meet the requirements of the Company under the provisions of this regulation. This information should include items such as:

.1 parties responsible for appointing shipboard personnel, such as ship management companies, manning agents, contractors, concessionaries (for example, retail sales outlets, casinos, etc.);

.2 parties responsible for deciding the employment of the ship, including time or bareboat charterer(s) or any other entity acting in such capacity; and

.3 in cases when the ship is employed under the terms of a charter party, the contact details of those parties, including time or voyage charterers.

6.2 In accordance with regulation XI-2/5, the Company is obliged to update and keep this information current as and when changes occur.

6.3 This information should be in English, French or Spanish language.

6.4 With respect to ships constructed before 1 July 2004, this information should reflect the actual condition on that date.

6.5 With respect to ships constructed on or after 1 July 2004 and for ships constructed before 1 July 2004 which were out of service on 1 July 2004, the information should be provided as from the date of entry of the ship into service and should reflect the actual condition on that date.

6.6 After 1 July 2004, when a ship is withdrawn from service, the information should be provided as from the date of re-entry of the ship into service and should reflect the actual condition on that date.

6.7 Previously provided information that does not relate to the actual condition on that date need not be retained on board.

6.8 When the responsibility for the operation of the ship is assumed by another Company, the information relating to the Company which operated the ship is not required to be left on board.

In addition, other relevant guidance is provided under sections 8, 9 and 13.

7 SHIP SECURITY

Relevant guidance is provided under sections 8, 9 and 13.

8 SHIP SECURITY ASSESSMENT

Security assessment

8.1 The company security officer (CSO) is responsible for ensuring that a ship security assessment (SSA) is carried out for each of the ships in the Company's fleet which is required to comply with the provisions of chapter XI-2 and part A of this Code for which the CSO is responsible. While the CSO need not necessarily personally undertake all the duties associated with the post, the ultimate responsibility for ensuring that they are properly performed remains with the individual CSO.

8.2 Prior to commencing the SSA, the CSO should ensure that advantage is taken of information available on the assessment of threat for the ports at which the ship will call or at which passengers embark or disembark and about the port facilities and their protective measures. The CSO should study previous reports on similar security needs. Where feasible, the CSO should meet with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the assessment. The CSO should follow any specific guidance offered by the Contracting Governments.

8.3 A SSA should address the following elements on board or within the ship:

.1 physical security;

.2 structural integrity;

.3 personnel protection systems;

.4 procedural policies;

.5 radio and telecommunication systems, including computer systems and networks; and

.6 other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations on board the ship or within a port facility.

8.4 Those involved in conducting a SSA should be able to draw upon expert assistance in relation to:

.1 knowledge of current security threats and patterns;

.2 recognition and detection of weapons, dangerous substances and devices;

.3 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.4 techniques used to circumvent security measures;

.5 methods used to cause a security incident;

.6 effects of explosives on ship's structures and equipment;

.7 ship security;

.8 ship/port interface business practices;

.9 contingency planning, emergency preparedness and response;

.10 physical security;

.11 radio and telecommunications systems, including computer systems and networks;

.12 marine engineering; and

.13 ship and port operations.

8.5 The CSO should obtain and record the information required to conduct an assessment, including:

.1 the general layout of the ship;

.2 the location of areas which should have restricted access, such as navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2, etc.;

.3 the location and function of each actual or potential access point to the ship;

.4 changes in the tide which may have an impact on the vulnerability or security of the ship;

.5 the cargo spaces and stowage arrangements;

.6 the locations where the ship's stores and essential maintenance equipment is stored;

.7 the locations where unaccompanied baggage is stored;

.8 the emergency and stand-by equipment available to maintain essential services;

.9 the number of ship's personnel, any existing security duties and any existing training requirement practises of the Company;

.10 existing security and safety equipment for the protection of passengers and ship's personnel;

.11 escape and evacuation routes and assembly stations which have to be maintained to ensure the orderly and safe emergency evacuation of the ship;

.12 existing agreements with private security companies providing ship/water-side security services; and

.13 existing security measures and procedures in effect, including inspection and, control procedures, identification systems, surveillance and monitoring equipment, personnel identification documents and communication, alarms, lighting, access control and other appropriate systems.

8.6 The SSA should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might seek to breach security. This includes points of access available to individuals having legitimate access as well as those who seek to obtain unauthorized entry.

8.7 The SSA should consider the continuing relevance of the existing security measures and guidance, procedures and operations, under both routine and emergency conditions, and should determine security guidance including:

.1 the restricted areas;

.2 the response procedures to fire or other emergency conditions;

.3 the level of supervision of the ship's personnel, passengers, visitors, vendors, repair technicians, dock workers, etc.;

.4 the frequency and effectiveness of security patrols;

.5 the access control systems, including identification systems;

.6 the security communications systems and procedures;

.7 the security doors, barriers and lighting; and

.8 the security and surveillance equipment and systems, if any.

8.8 The SSA should consider the persons, activities, services and operations that it is important to protect. This includes:

.1 the ship's personnel;

.2 passengers, visitors, vendors, repair technicians, port facility personnel, etc.;

.3 the capacity to maintain safe navigation and emergency response;

.4 the cargo, particularly dangerous goods or hazardous substances;

.5 the ship's stores;

.6 the ship security communication equipment and systems, if any; and

.7 the ship's security surveillance equipment and systems, if any.

8.9 The SSA should consider all possible threats, which may include the following types of security incidents:

.1 damage to, or destruction of, the ship or of a port facility, e.g. by explosive devices, arson, sabotage or vandalism;

.2 hijacking or seizure of the ship or of persons on board;

.3 tampering with cargo, essential ship equipment or systems or ship's stores;

.4 unauthorized access or use, including presence of stowaways;

.5 smuggling weapons or equipment, including weapons of mass destruction;

.6 use of the ship to carry those intending to cause a security incident and/or their equipment;

.7 use of the ship itself as a weapon or as a means to cause damage or destruction;

.8 attacks from seaward whilst at berth or at anchor; and

.9 attacks whilst at sea.

8.10 The SSA should take into account all possible vulnerabilities, which may include:

.1 conflicts between safety and security measures;

.2 conflicts between shipboard duties and security assignments;

.3 watchkeeping duties, number of ship's personnel, particularly with implications on crew fatigue, alertness and performance;

.4 any identified security training deficiencies; and

.5 any security equipment and systems, including communication systems.

8.11 The CSO and ship security officer (SSO) should always have regard to the effect that security measures may have on ship's personnel who will remain on the ship for long periods. When developing security measures, particular consideration should be given to the convenience, comfort and personal privacy of the ship's personnel and their ability to maintain their effectiveness over long periods.

8.12 Upon completion of the SSA, a report shall be prepared, consisting of a summary of how the assessment was conducted, a description of each vulnerability found during the assessment and a description of countermeasures that could be used to address each vulnerability. The report shall be protected from unauthorized access or disclosure.

8.13 If the SSA has not been carried out by the Company, the report of the SSA should be reviewed and accepted by the CSO.

On-scene security survey

8.14 The on-scene security survey is an integral part of any SSA. The on-scene security survey should examine and evaluate existing shipboard protective measures, procedures and operations for:

.1 ensuring the performance of all ship security duties;

.2 monitoring restricted areas to ensure that only authorized persons have access;

.3 controlling access to the ship, including any identification systems;

.4 monitoring of deck areas and areas surrounding the ship;

.5 controlling the embarkation of persons and their effects (accompanied and unaccompanied baggage and ship's personnel personal effects);

.6 supervising the handling of cargo and the delivery of ship's stores; and

.7 ensuring that ship security communication, information, and equipment are readily available.

9 SHIP SECURITY PLAN

General

9.1 The company security officer (CSO) has the responsibility of ensuring that a ship security plan (SSP) is prepared and submitted for approval. The content of each individual SSP should vary depending on the particular ship it covers. The ship security assessment (SSA) will have identified the particular features of the ship and the potential threats and vulnerabilities. The preparation of the SSP will require these features to be addressed in detail. Administrations may prepare advice on the preparation and content of a SSP.

9.2 All SSPs should:

.1 detail the organizational structure of security for the ship;

.2 detail the ship's relationships with the Company, port facilities, other ships and relevant authorities with security responsibility;

.3 detail the communication systems to allow effective continuous communication within the ship and between the ship and others, including port facilities;

.4 detail the basic security measures for security level 1, both operational and physical, that will always be in place;

.5 detail the additional security measures that will allow the ship to progress without delay to security level 2 and, when necessary, to security level 3;

.6 provide for regular review, or audit, of the SSP and for its amendment in response to experience or changing circumstances; and

.7 detail reporting procedures to the appropriate Contracting Government's contact points.

9.3 Preparation of an effective SSP should rest on a thorough assessment of all issues that relate to the security of the ship, including, in particular, a thorough appreciation of the physical and operational characteristics, including the voyage pattern, of the individual ship.

9.4 All SSPs should be approved by, or on behalf of, the Administration. If an Administration uses a recognized security organization (RSO) to review or approve the SSP, that RSO should not be associated with any other RSO that prepared, or assisted in the preparation of, the plan.

9.5 CSOs and SSOs should develop procedures to:

.1 assess the continuing effectiveness of the SSP; and

.2 prepare amendments of the plan subsequent to its approval.

9.6 The security measures included in the SSP should be in place when the initial verification for compliance with the requirements of chapter XI-2 and part A of this Code will be carried out. Otherwise the process of issue to the ship of the required International Ship Security Certificate cannot be carried out. If there is any subsequent failure of security equipment or systems, or suspension of a security measure for whatever reason, equivalent temporary security measures should be adopted, notified to, and agreed by the Administration.

Organization and performance of ship security duties

9.7 In addition to the guidance given in paragraph 9.2, the SSP should establish the following, which relate to all security levels:

.1 the duties and responsibilities of all shipboard personnel with a security role;

.2 the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;

.3 the procedures needed to assess the continuing effectiveness of security procedures and any security and surveillance equipment and systems, including procedures for identifying and responding to equipment or systems failure or malfunction;

.4 the procedures and practices to protect security-sensitive information held in paper or electronic format;

.5 the type and maintenance requirements of security and surveillance equipment and systems, if any;

.6 the procedures to ensure the timely submission, and assessment, of reports relating to possible breaches of security or security concerns; and

.7 procedures to establish, maintain and update an inventory of any dangerous goods or hazardous substances carried on board, including their location.

9.8 The remainder of section 9 addresses specifically the security measures that could be taken at each security level covering:

.1 access to the ship by ship's personnel, passengers, visitors, etc.;

.2 restricted areas on the ship;

.3 handling of cargo;

.4 delivery of ship's stores;

.5 handling unaccompanied baggage; and

.6 monitoring the security of the ship.

Access to the ship

9.9 The SSP should establish the security measures covering all means of access to the ship identified in the SSA. This should include any:

.1 access ladders;

.2 access gangways;

.3 access ramps;

.4 access doors, sidescuttles, windows and ports;

.5 mooring lines and anchor chains; and

.6 cranes and hoisting gear.

9.10 For each of these the SSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the SSP should establish the type of restriction or prohibition to be applied and the means of enforcing them.

9.11 The SSP should establish for each security level the means of identification required to allow access to the ship and for individuals to remain on the ship without challenge. This may involve developing an appropriate identification system allowing for permanent and temporary identifications, for ship's personnel and visitors respectively. Any ship identification system should, when it is practicable to do so, be co-ordinated with that applying to the port facility. Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted access to restricted areas unless supervised. The SSP should establish provisions to ensure that the identification systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

9.12 Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the ship and their attempt to obtain

access should be reported, as appropriate, to the SSO, the CSO, the port facility security officer (PFSO) and to the national or local authorities with security responsibilities.

9.13 The SSP should establish the frequency of application of any access controls, particularly if they are to be applied on a random, or occasional, basis.

Security level 1

9.14 At security level 1, the SSP should establish the security measures to control access to the ship, where the following may be applied:

.1 checking the identity of all persons seeking to board the ship and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders, etc.;

.2 in liaison with the port facility, the ship should ensure that designated secure areas are established in which inspections and searching of persons, baggage (including carry-on items), personal effects, vehicles and their contents can take place;

.3 in liaison with the port facility, the ship should ensure that vehicles destined to be loaded on board car carriers, ro-ro and other passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP;

.4 segregating checked persons and their personal effects from unchecked persons and their personal effects;

.5 segregating embarking from disembarking passengers;

.6 identifying access points that should be secured or attended to prevent unauthorized access;

.7 securing, by locking or other means, access to unattended spaces adjoining areas to which passengers and visitors have access; and

.8 providing security briefings to all ship personnel on possible threats, the procedures for reporting suspicious persons, objects or activities and the need for vigilance.

9.15 At security level 1, all those seeking to board a ship should be liable to search. The frequency of such searches, including random searches, should be specified in the approved SSP and should be specifically approved by the Administration. Such searches may best be undertaken by the port facility in close co-operation with the ship and in close proximity to it. Unless there are clear security grounds for doing so, members of the ship's personnel should not be required to search their colleagues or their personal effects. Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.

Security level 2

9.16 At security level 2, the SSP should establish the security measures to be applied to protect against a heightened risk of a security incident to ensure higher vigilance and tighter control, which may include:

.1 assigning additional personnel to patrol deck areas during silent hours to deter unauthorized access;

.2 limiting the number of access points to the ship, identifying those to be closed and the means of adequately securing them;

.3 deterring waterside access to the ship, including, for example, in liaison with the port facility, provision of boat patrols;

.4 establishing a restricted area on the shore side of the ship, in close co-operation with the port facility;

.5 increasing the frequency and detail of searches of persons, personal effects, and vehicles being embarked or loaded onto the ship;

.6 escorting visitors on the ship;

.7 providing additional specific security briefings to all ship personnel on any identified threats, re-emphasizing the procedures for reporting suspicious persons, objects, or activities and stressing the need for increased vigilance; and

.8 carrying out a full or partial search of the ship.

Security level 3

9.17 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 limiting access to a single, controlled, access point;

.2 granting access only to those responding to the security incident or threat thereof;

.3 directing persons on board;

.4 suspension of embarkation or disembarkation;

.5 suspension of cargo handling operations, deliveries, etc.;

.6 evacuation of the ship;

.7 movement of the ship; and

.8 preparing for a full or partial search of the ship.

Restricted areas on the ship

9.18 The SSP should identify the restricted areas to be established on the ship, specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. The purposes of restricted areas are to:

.1 prevent unauthorized access;

.2 protect passengers, ship's personnel, and personnel from port facilities or other agencies authorized to be on board the ship;

.3 protect security-sensitive areas within the ship; and

.4 protect cargo and ship's stores from tampering.

9.19 The SSP should ensure that there are clearly established policies and practices to control access to all restricted areas.

9.20 The SSP should provide that all restricted areas should be clearly marked, indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

9.21 Restricted areas may include:

.1 navigation bridge, machinery spaces of category A and other control stations as defined in chapter II-2;

.2 spaces containing security and surveillance equipment and systems and their controls and lighting system controls;

.3 ventilation and air-conditioning systems and other similar spaces;

.4 spaces with access to potable water tanks, pumps, or manifolds;

.5 spaces containing dangerous goods or hazardous substances;

.6 spaces containing cargo pumps and their controls;

.7 cargo spaces and spaces containing ship's stores;

.8 crew accommodation; and

.9 any other areas as determined by the CSO, through the SSA, to which access must be restricted to maintain the security of the ship.

Security level 1

9.22 At security level 1, the SSP should establish the security measures to be applied to restricted areas, which may include:

.1 locking or securing access points;

.2 using surveillance equipment to monitor the areas;

.3 using guards or patrols; and

.4 using automatic intrusion-detection devices to alert the ship's personnel of unauthorized access.

Security level 2

9.23 At security level 2, the frequency and intensity of the monitoring of, and control of access to, restricted areas should be increased to ensure that only authorized persons have access. The SSP should establish the additional security measures to be applied, which may include:

.1 establishing restricted areas adjacent to access points;

.2 continuously monitoring surveillance equipment; and

.3 dedicating additional personnel to guard and patrol restricted areas.

Security level 3

9.24 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 setting up of additional restricted areas on the ship in proximity to the security incident, or the believed location of the security threat, to which access is denied; and

.2 searching of restricted areas as part of a search of the ship.

Handling of cargo

9.25 The security measures relating to cargo handling should:

.1 prevent tampering; and

.2 prevent cargo that is not meant for carriage from being accepted and stored on board the ship.

9.26 The security measures, some of which may have to be applied in liaison with the port facility, should include inventory control procedures at access points to the ship. Once on board the ship, cargo should be capable of being identified as having been approved for loading onto the ship. In addition, security measures should be developed to ensure that cargo, once on board, is not tampered with.

Security level 1

9.27 At security level 1, the SSP should establish the security measures to be applied during cargo handling, which may include:

.1 routine checking of cargo, cargo transport units and cargo spaces prior to, and during, cargo handling operations;

.2 checks to ensure that cargo being loaded matches the cargo documentation;

.3 ensuring, in liaison with the port facility, that vehicles to be loaded on board car-carriers, ro-ro and passenger ships are subjected to search prior to loading, in accordance with the frequency required in the SSP; and

.4 checking of seals or other methods used to prevent tampering.

9.28 Checking of cargo may be accomplished by the following means:

.1 visual and physical examination; and

.2 using scanning/detection equipment, mechanical devices, or dogs.

9.29 When there are regular or repeated cargo movements, the CSO or SSO may, in consultation with the port facility, agree arrangements with shippers or others responsible for such cargo covering off-site checking, sealing, scheduling, supporting documentation, etc. Such arrangements should be communicated to and agreed with the PFSO concerned.

Security level 2

9.30 At security level 2, the SSP should establish the additional security measures to be applied during cargo handling, which may include:

.1 detailed checking of cargo, cargo transport units and cargo spaces;

.2 intensified checks to ensure that only the intended cargo is loaded;

.3 intensified searching of vehicles to be loaded on car carriers, ro-ro and passenger ships; and

.4 increased frequency and detail in checking of seals or other methods used to prevent tampering.

9.31 Detailed checking of cargo may be accomplished by the following means:

.1 increasing the frequency and detail of visual and physical examination;

.2 increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and

.3 co-ordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures.

Security level 3

9.32 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 suspending the loading or unloading of cargo; and

.2 verifying the inventory of dangerous goods and hazardous substances carried on board, if any, and their location.

Delivery of ship's stores

9.33 The security measures relating to the delivery of ship's stores should:

.1 ensure checking of ship's stores and package integrity;

.2 prevent ship's stores from being accepted without inspection;

.3 prevent tampering; and

.4 prevent ship's stores from being accepted unless ordered.

9.34 For ships regularly using the port facility, it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

Security level 1

9.35 At security level 1, the SSP should establish the security measures to be applied during delivery of ship's stores, which may include:

.1 checking to ensure stores match the order prior to being loaded on board; and

.2 ensuring immediate secure stowage of ship's stores.

Security level 2

9.36 At security level 2, the SSP should establish the additional security measures to be applied during delivery of ship's stores by exercising checks prior to receiving stores on board and intensifying inspections.

Security level 3

9.37 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 subjecting ship's stores to more extensive checking;

.2 preparation for restriction or suspension of handling of ship's stores; and

.3 refusal to accept ship's stores on board the ship.

Handling unaccompanied baggage

9.38 The SSP should establish the security measures to be applied to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before it is accepted on board the ship. It

is not envisaged that such baggage will be subjected to screening by both the ship and the port facility, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility. Close co-operation with the port facility is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

Security level 1

9.39 At security level 1, the SSP should establish the security measures to be applied when handling unaccompanied baggage to ensure that unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

Security level 2

9.40 At security level 2, the SSP should establish the additional security measures to be applied when handling unaccompanied baggage, which should include 100 percent x-ray screening of all unaccompanied baggage.

Security level 3

9.41 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;

.2 preparation for restriction or suspension of handling of unaccompanied baggage; and

.3 refusal to accept unaccompanied baggage on board the ship.

Monitoring the security of the ship

9.42 The ship should have the capability to monitor the ship, the restricted areas on board and areas surrounding the ship. Such monitoring capabilities may include use of:

.1 lighting;

.2 watchkeepers, security guards and deck watches, including patrols; and

.3 automatic intrusion-detection devices and surveillance equipment.

9.43 When used, automatic intrusion-detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

9.44 The SSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather conditions or of power disruptions.

Security level 1

9.45 At security level 1, the SSP should establish the security measures to be applied, which may be a combination of lighting, watchkeepers, security guards or use of security and surveillance equipment to allow ship's security personnel to observe the ship in general, and barriers and restricted areas in particular.

9.46 The ship's deck and access points to the ship should be illuminated during hours of darkness and periods of low visibility while conducting ship/port interface activities or at a port facility or anchorage when necessary. While under way, when necessary, ships should use the maximum lighting available consistent with safe navigation, having regard to the provisions of the International Regulations for the Prevention of Collisions at Sea in force. The following should be considered when establishing the appropriate level and location of lighting:

.1 the ship's personnel should be able to detect activities beyond the ship, on both the shore side and the water side;

.2 coverage should include the area on and around the ship;

.3 coverage should facilitate personnel identification at access points; and

.4 coverage may be provided through co-ordination with the port facility.

Security level 2

9.47 At security level 2, the SSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capabilities, which may include:

.1 increasing the frequency and detail of security patrols;

.2 increasing the coverage and intensity of lighting or the use of security and surveillance equipment;

.3 assigning additional personnel as security look-outs; and

.4 ensuring co-ordination with water-side boat patrols, and foot or vehicle patrols on the shore side, when provided.

9.48 Additional lighting may be necessary to protect against a heightened risk of a security incident. When necessary, the additional lighting requirements may be accomplished by co-ordinating with the port facility to provide additional shoreside lighting.

Security level 3

9.49 At security level 3, the ship should comply with the instructions issued by those responding to the security incident or threat thereof. The SSP should detail the security measures which could be taken by the ship, in close co-operation with those responding and the port facility, which may include:

.1 switching on of all lighting on, or illuminating the vicinity of, the ship;

.2 switching on of all on-board surveillance equipment capable of recording activities on, or in the vicinity of, the ship;

.3 maximizing the length of time such surveillance equipment can continue to record;

.4 preparation for underwater inspection of the hull of the ship; and

.5 initiation of measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.

Differing security levels

9.50 The SSP should establish details of the procedures and security measures the ship could adopt if the ship is at a higher security level than that applying to a port facility.

Activities not covered by the Code

9.51 The SSP should establish details of the procedures and security measures the ship should apply when:

.1 it is at a port of a State which is not a Contracting Government;

.2 it is interfacing with a ship to which this Code does not apply;

.3 it is interfacing with fixed or floating platforms or a mobile drilling unit on location; or

.4 it is interfacing with a port or port facility which is not required to comply with chapter XI-2 and part A of this Code.

Declarations of Security

9.52 The SSP should detail how requests for Declarations of Security from a port facility will be handled and the circumstances under which the ship itself should request a DoS.

Audit and review

9.53 The SSP should establish how the CSO and the SSO intend to audit the continued effectiveness of the SSP and the procedure to be followed to review, update or amend the SSP.

10 RECORDS

General

10.1 Records should be available to duly authorized officers of Contracting Governments to verify that the provisions of ship security plans are being implemented.

10.2 Records may be kept in any format but should be protected from unauthorized access or disclosure.

11 COMPANY SECURITY OFFICER

Relevant guidance is provided under sections 8, 9 and 13.

12 SHIP SECURITY OFFICER

Relevant guidance is provided under sections 8, 9 and 13.

13 TRAINING, DRILLS AND EXERCISES ON SHIP SECURITY

Training

13.1 The company security officer (CSO) and appropriate shore-based Company personnel, and the ship security officer (SSO), should have knowledge of, and receive training, in some or all of the following, as appropriate:

.1 security administration;

.2 relevant international conventions, codes and recommendations;

.3 relevant Government legislation and regulations;

.4 responsibilities and functions of other security organizations;

.5 methodology of ship security assessment;

.6 methods of ship security surveys and inspections;

.7 ship and port operations and conditions;

.8 ship and port facility security measures;

.9 emergency preparedness and response and contingency planning;

.10 instruction techniques for security training and education, including security measures and procedures;

.11 handling sensitive security-related information and security-related communications;

.12 knowledge of current security threats and patterns;

.13 recognition and detection of weapons, dangerous substances and devices;

.14 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.15 techniques used to circumvent security measures;

.16 security equipment and systems and their operational limitations;

.17 methods of conducting audits, inspection, control and monitoring;

.18 methods of physical searches and non-intrusive inspections;

.19 security drills and exercises, including drills and exercises with port facilities; and

.20 assessment of security drills and exercises.

13.2 In addition, the SSO should have adequate knowledge of, and receive training in, some or all of the following, as appropriate:

.1 the layout of the ship;

.2 the ship security plan and related procedures (including scenario-based training on how to respond);

.3 crowd management and control techniques;

.4 operations of security equipment and systems; and

.5 testing, calibration and at-sea maintenance of security equipment and systems.

13.3 Shipboard personnel having specific security duties should have sufficient knowledge and ability to perform their assigned duties, including, as appropriate:

.1 knowledge of current security threats and patterns;

.2 recognition and detection of weapons, dangerous substances and devices;

.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;

.4 techniques used to circumvent security measures;

.5 crowd management and control techniques;

.6 security-related communications;

.7 knowledge of the emergency procedures and contingency plans;

.8 operations of security equipment and systems;

.9 testing, calibration and at-sea maintenance of security equipment and systems;

.10 inspection, control, and monitoring techniques; and

.11 methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

13.4 All other shipboard personnel should have sufficient knowledge of and be familiar with relevant provisions of the ship security plan (SSP), including:

.1 the meaning and the consequential requirements of the different security levels;

.2 knowledge of the emergency procedures and contingency plans;

.3 recognition and detection of weapons, dangerous substances and devices;

.4 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security; and

.5 techniques used to circumvent security measures.

Drills and exercises

13.5 The objective of drills and exercises is to ensure that shipboard personnel are proficient in all assigned security duties at all security levels and the identification of any security-related deficiencies which need to be addressed.

13.6 To ensure the effective implementation of the provisions of the ship security plan, drills should be conducted at least once every three months. In addition, in cases where more than 25 percent of the ship's personnel has been changed, at any one time, with personnel that has not previously participated in any drill on that ship within the last 3 months, a drill should be conducted within one week of the change. These drills should test individual elements of the plan such as those security threats listed in paragraph 8.9.

13.7 Various types of exercises, which may include participation of company security officers, port facility security officers, relevant authorities of Contracting Governments as well as ship security officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. These exercises should test communications, co-ordination, resource availability, and response. These exercises may be:

.1 full-scale or live;

.2 tabletop simulation or seminar; or

.3 combined with other exercises held, such as search and rescue or emergency response exercises.

13.8 Company participation in an exercise with another Contracting Government should be recognized by the Administration.

14 PORT FACILITY SECURITY

Relevant guidance is provided under sections 15, 16 and 18.

15 PORT FACILITY SECURITY ASSESSMENT

General

15.1 The port facility security assessment (PFSA) may be conducted by a recognized security organization (RSO). However, approval of a completed PFSA should only be given by the relevant Contracting Government.

15.2 If a Contracting Government uses a RSO to review or verify compliance of the PFSA, the RSO should not be associated with any other RSO that prepared or assisted in the preparation of that assessment.

15.3 A PFSA should address the following elements within a port facility:

.1 physical security;

.2 structural integrity;

.3 personnel protection systems;

.4 procedural policies;

.5 radio and telecommunication systems, including computer systems and networks;

.6 relevant transportation infrastructure;

.7 utilities; and

.8 other areas that may, if damaged or used for illicit observation, pose a risk to persons, property, or operations within the port facility.

15.4 Those involved in a PFSA should be able to draw upon expert assistance in relation to:

.1 knowledge of current security threats and patterns;

.2 recognition and detection of weapons, dangerous substances and devices;

.3 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten security;

.4 techniques used to circumvent security measures;

.5 methods used to cause a security incident;

.6 effects of explosives on structures and port facility services;

.7 port facility security;

.8 port business practices;

.9 contingency planning, emergency preparedness and response;

.10 physical security measures, e.g. fences;

.11 radio and telecommunications systems, including computer systems and networks;

.12 transport and civil engineering; and

.13 ship and port operations.

Identification and evaluation of important assets and infrastructure it is important to protect

15.5 The identification and evaluation of important assets and infrastructure is a process through which the relative importance of structures and installations to the functioning of the port facility can be established. This identification and evaluation process is important because it provides a basis for focusing mitigation strategies on those assets and structures which it is more important to protect from a security incident. This process should take into account potential loss of life, the economic significance of the port, symbolic value, and the presence of Government installations.

15.6 Identification and evaluation of assets and infrastructure should be used to prioritize their relative importance for protection. The primary concern should be avoidance of death or injury. It is also important to consider whether the port facility, structure or installation can continue to function without the asset, and the extent to which rapid re-establishment of normal functioning is possible.

15.7 Assets and infrastructure that should be considered important to protect may include:

.1 accesses, entrances, approaches, and anchorages, manoeuvring and berthing areas;

.2 cargo facilities, terminals, storage areas, and cargo handling equipment;

.3 systems such as electrical distribution systems, radio and telecommunication systems and computer systems and networks;

.4 port vessel traffic management systems and aids to navigation;

.5 power plants, cargo transfer piping, and water supplies;

.6 bridges, railways, roads;

.7 port service vessels, including pilot boats, tugs, lighters, etc.;

.8 security and surveillance equipment and systems; and

.9 the waters adjacent to the port facility.

15.8 The clear identification of assets and infrastructure is essential to the evaluation of the port facility's security requirements, the prioritization of protective measures, and decisions concerning the allocation of resources to better protect the port facility. The process may involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

Identification of the possible threats to the assets and infrastructure and the likelihood of their occurrence, in order to establish and prioritize security measures

15.9 Possible acts that could threaten the security of assets and infrastructure, and the methods of carrying out those acts, should be identified to evaluate the vulnerability of a given asset or location to a security incident, and to establish and prioritize security requirements to enable planning and resource allocations. Identification and evaluation of each potential act and its method should be based on various factors, including threat assessments by Government agencies. By identifying and assessing threats, those conducting the assessment do not have to rely on worst-case scenarios to guide planning and resource allocations.

15.10 The PFSA should include an assessment undertaken in consultation with the relevant national security organizations to determine:

.1 any particular aspects of the port facility, including the vessel traffic using the facility, which make it likely to be the target of an attack;

.2 the likely consequences in terms of loss of life, damage to property and economic disruption, including disruption to transport systems, of an attack on, or at, the port facility;

.3 the capability and intent of those likely to mount such an attack; and

.4 the possible type, or types, of attack,

producing an overall assessment of the level of risk against which security measures have to be developed.

15.11 The PFSA should consider all possible threats, which may include the following types of security incidents:

.1 damage to, or destruction of, the port facility or of the ship, e.g. by explosive devices, arson, sabotage or vandalism;

.2 hijacking or seizure of the ship or of persons on board;

.3 tampering with cargo, essential ship equipment or systems or ship's stores;

.4 unauthorized access or use, including presence of stowaways;

.5 smuggling weapons or equipment, including weapons of mass destruction;

.6 use of the ship to carry those intending to cause a security incident and their equipment;

.7 use of the ship itself as a weapon or as a means to cause damage or destruction;

.8 blockage of port entrances, locks, approaches, etc.; and

.9 nuclear, biological and chemical attack.

15.12 The process should involve consultation with the relevant authorities relating to structures adjacent to the port facility which could cause damage within the facility or be used for the purpose of causing damage to the facility or for illicit observation of the facility or for diverting attention.

Identification, selection, and prioritization of countermeasures and procedural changes and their level of effectiveness in reducing vulnerability

15.13 The identification and prioritization of countermeasures is designed to ensure that the most effective security measures are employed to reduce the vulnerability of a port facility or ship/port interface to the possible threats.

15.14 Security measures should be selected on the basis of factors such as whether they reduce the probability of an attack and should be evaluated using information that includes:

.1 security surveys, inspections and audits;

.2 consultation with port facility owners and operators, and owners/operators of adjacent structures if appropriate;

.3 historical information on security incidents; and

.4 operations within the port facility.

Identification of vulnerabilities

15.15 Identification of vulnerabilities in physical structures, personnel protection systems, processes, or other areas that may lead to a security incident can be used to establish options to eliminate or mitigate those vulnerabilities. For example, an analysis might reveal vulnerabilities in a port facility's security systems or unprotected infrastructure such as water supplies, bridges, etc. that could be resolved through physical measures, e.g. permanent barriers, alarms, surveillance equipment, etc.

15.16 Identification of vulnerabilities should include consideration of:

.1 water-side and shore-side access to the port facility and ships berthing at the facility;

.2 structural integrity of the piers, facilities, and associated structures;

.3 existing security measures and procedures, including identification systems;

.4 existing security measures and procedures relating to port services and utilities;

.5 measures to protect radio and telecommunication equipment, port services and utilities, including computer systems and networks;

.6 adjacent areas that may be exploited during, or for, an attack;

.7 existing agreements with private security companies providing water-side/shore-side security services;

.8 any conflicting policies between safety and security measures and procedures;

.9 any conflicting port facility and security duty assignments;

.10 any enforcement and personnel constraints;

.11 any deficiencies identified during training and drills; and

.12 any deficiencies identified during daily operation, following incidents or alerts, the report of security concerns, the exercise of control measures, audits, etc.

16 PORT FACILITY SECURITY PLAN

General

16.1 Preparation of the port facility security plan (PFSP) is the responsibility of the port facility security officer (PFSO). While the PFSO need not necessarily personally undertake all the duties associated with the post, the ultimate responsibility for ensuring that they are properly performed remains with the individual PFSO.

16.2 The content of each individual PFSP should vary depending on the particular circumstances of the port facility, or facilities, it covers. The port facility security assessment (PFSA) will have identified the particular features of the port facility, and of the potential security risks, that have led to the need to appoint a PFSO and to prepare a PFSP. The preparation of the PFSP will require these features, and other local or national security considerations, to be addressed in the PFSP and for appropriate security measures to be established so as to minimise the likelihood of a breach of security and the consequences of potential risks. Contracting Governments may prepare advice on the preparation and content of a PFSP.

16.3 All PFSPs should:

.1 detail the security organization of the port facility;

.2 detail the organization's links with other relevant authorities and the necessary communication systems to allow the effective continuous operation of the organization and its links with others, including ships in port;

.3 detail the basic security level 1 measures, both operational and physical, that will be in place;

.4 detail the additional security measures that will allow the port facility to progress without delay to security level 2 and, when necessary, to security level 3;

.5 provide for regular review, or audit, of the PFSP and for its amendment in response to experience or changing circumstances; and

.6 detail reporting procedures to the appropriate Contracting Government's contact points.

16.4 Preparation of an effective PFSP will rest on a thorough assessment of all issues that relate to the security of the port facility, including, in particular, a thorough appreciation of the physical and operational characteristics of the individual port facility.

16.5 Contracting Governments should approve the PFSPs of the port facilities under their jurisdiction. Contracting Governments should develop procedures to assess the continuing effectiveness of each PFSP and may require amendment of the PFSP prior to its initial approval or subsequent to its approval. The PFSP should make provision for the retention of records of security incidents and threats, reviews, audits, training, drills and exercises as evidence of compliance with those requirements.

16.6 The security measures included in the PFSP should be in place within a reasonable period of the PFSP's approval and the PFSP should establish when each measure will be in place. If there is likely to be any delay in their provision, this should be discussed with the Contracting Government responsible for approval of the PFSP and satisfactory alternative temporary security measures that provide an equivalent level of security should be agreed to cover any interim period.

16.7 The use of firearms on or near ships and in port facilities may pose particular and significant safety risks, in particular in connection with certain dangerous or hazardous substances, and should be considered very carefully. In the event that a Contracting Government decides that it is necessary to use armed personnel in these areas, that Contracting Government

should ensure that these personnel are duly authorized and trained in the use of their weapons and that they are aware of the specific risks to safety that are present in these areas. If a Contracting Government authorizes the use of firearms they should issue specific safety guidelines on their use. The PFSP should contain specific guidance on this matter, in particular with regard its application to ships carrying dangerous goods or hazardous substances.

Organization and performance of port facility security duties

16.8 In addition to the guidance given under paragraph 16.3, the PFSP should establish the following, which relate to all security levels:

.1 the role and structure of the port facility security organization;

.2 the duties, responsibilities and training requirements of all port facility personnel with a security role and the performance measures needed to allow their individual effectiveness to be assessed;

.3 the port facility security organization's links with other national or local authorities with security responsibilities;

.4 the communication systems provided to allow effective and continuous communication between port facility security personnel, ships in port and, when appropriate, with national or local authorities with security responsibilities;

.5 the procedures or safeguards necessary to allow such continuous communications to be maintained at all times;

.6 the procedures and practices to protect security-sensitive information held in paper or electronic format;

.7 the procedures to assess the continuing effectiveness of security measures, procedures and equipment, including identification of, and response to, equipment failure or malfunction;

.8 the procedures to allow the submission, and assessment, of reports relating to possible breaches of security or security concerns;

.9 procedures relating to cargo handling;

.10 procedures covering the delivery of ship's stores;

.11 the procedures to maintain, and update, records of dangerous goods and hazardous substances and their location within the port facility;

.12 the means of alerting and obtaining the services of waterside patrols and specialist search teams, including bomb searches and underwater searches;

.13 the procedures for assisting ship security officers in confirming the identity of those seeking to board the ship when requested; and

.14 the procedures for facilitating shore leave for ship's personnel or personnel changes, as well as access of visitors to the ship, including representatives of seafarers' welfare and labour organizations.

16.9 The remainder of section 16 addresses specifically the security measures that could be taken at each security level covering:

.1 access to the port facility;

.2 restricted areas within the port facility;

.3 handling of cargo;

.4 delivery of ship's stores;

.5 handling unaccompanied baggage; and

.6 monitoring the security of the port facility.

Access to the port facility

16.10 The PFSP should establish the security measures covering all means of access to the port facility identified in the PFSA.

16.11 For each of these the PFSP should identify the appropriate locations where access restrictions or prohibitions should be applied for each of the security levels. For each security level the PFSP should specify the type of restriction or prohibition to be applied and the means of enforcing them.

16.12 The PFSP should establish for each security level the means of identification required to allow access to the port facility and for individuals to remain within the port facility without challenge. This may involve developing an appropriate identification system, allowing for permanent and temporary identifications, for port facility personnel and for visitors respectively. Any port facility identification system should, when it is practicable to do so, be co-ordinated with that applying to ships that regularly use the port facility. Passengers should be able to prove their identity by boarding passes, tickets, etc., but should not be permitted access to restricted areas unless supervised. The PFSP should establish provisions to ensure that the identification systems are regularly updated, and that abuse of procedures should be subject to disciplinary action.

16.13 Those unwilling or unable to establish their identity and/or to confirm the purpose of their visit when requested to do so should be denied access to the port facility and their attempt to obtain access should be reported to the PFSO and to the national or local authorities with security responsibilities.

16.14 The PFSP should identify the locations where persons, personal effects, and vehicle searches are to be undertaken. Such locations should be covered to facilitate continuous operation, regardless of prevailing weather conditions, in accordance with the frequency laid down in the PFSP. Once subjected to search, persons, personal effects and vehicles should proceed directly to the restricted holding, embarkation or car loading areas.

16.15 The PFSP should establish separate locations for checked and unchecked persons and their effects and if possible separate areas for embarking/disembarking passengers, ship's personnel and their effects to ensure that unchecked persons are not able to come in contact with checked persons.

16.16 The PFSP should establish the frequency of application of any access controls, particularly if they are to be applied on a random, or occasional, basis.

Security level 1

16.17 At security level 1, the PFSP should establish the control points where the following security measures may be applied:

.1 restricted areas, which should be bounded by fencing or other barriers to a standard which should be approved by the Contracting Government;

.2 checking identity of all persons seeking entry to the port facility in connection with a ship, including passengers, ship's personnel and visitors, and confirming their reasons for doing so by checking, for example, joining instructions, passenger tickets, boarding passes, work orders, etc.;

.3 checking vehicles used by those seeking entry to the port facility in connection with a ship;

.4 verification of the identity of port facility personnel and those employed within the port facility and their vehicles;

.5 restricting access to exclude those not employed by the port facility or working within it, if they are unable to establish their identity;

.6 undertaking searches of persons, personal effects, vehicles and their contents; and

.7 identification of any access points not in regular use, which should be permanently closed and locked.

16.18 At security level 1, all those seeking access to the port facility should be liable to search. The frequency of such searches, including random searches, should be specified in the approved PFSP and should be specifically approved by the Contracting Government. Unless there are clear security grounds for doing so, members of the ship's personnel should not be required to search their colleagues or their personal effects. Any such search shall be undertaken in a manner which fully takes into account the human rights of the individual and preserves their basic human dignity.

Security level 2

16.19 At security level 2, the PFSP should establish the additional security measures to be applied, which may include:

.1 assigning additional personnel to guard access points and patrol perimeter barriers;

.2 limiting the number of access points to the port facility, and identifying those to be closed and the means of adequately securing them;

.3 providing for means of impeding movement through the remaining access points, e.g. security barriers;

.4 increasing the frequency of searches of persons, personal effects, and vehicles;

.5 denying access to visitors who are unable to provide a verifiable justification for seeking access to the port facility; and

.6 using patrol vessels to enhance water-side security.

Security level 3

16.20 At security level 3, the port facility should comply with instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include:

.1 suspension of access to all, or part, of the port facility;

.2 granting access only to those responding to the security incident or threat thereof;

.3 suspension of pedestrian or vehicular movement within all, or part, of the port facility;

.4 increased security patrols within the port facility, if appropriate;

.5 suspension of port operations within all, or part, of the port facility;

.6 direction of vessel movements relating to all, or part, of the port facility; and

.7 evacuation of all, or part, of the port facility.

Restricted areas within the port facility

16.21 The PFSP should identify the restricted areas to be established within the port facility and specify their extent, times of application, the security measures to be taken to control access to them and those to be taken to control activities within them. This should also include, in appropriate circumstances, measures to ensure that temporary restricted areas are security swept both before and after that area is established. The purpose of restricted areas is to:

.1 protect passengers, ship's personnel, port facility personnel and visitors, including those visiting in connection with a ship;

.2 protect the port facility;

.3 protect ships using, and serving, the port facility;

.4 protect security-sensitive locations and areas within the port facility;

.5 protect security and surveillance equipment and systems; and

.6 protect cargo and ship's stores from tampering.

16.22 The PFSP should ensure that all restricted areas have clearly established security measures to control:

.1 access by individuals;

.2 the entry, parking, loading and unloading of vehicles;

.3 movement and storage of cargo and ship's stores; and

.4 unaccompanied baggage or personal effects.

16.23 The PFSP should provide that all restricted areas should be clearly marked, indicating that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security.

16.24 When automatic intrusion-detection devices are installed they should alert a control centre which can respond to the triggering of an alarm.

16.25 Restricted areas may include:

.1 shore- and water-side areas immediately adjacent to the ship;

.2 embarkation and disembarkation areas, passenger and ship's personnel holding and processing areas, including search points;

.3 areas where loading, unloading or storage of cargo and stores is undertaken;

.4 locations where security-sensitive information, including cargo documentation, is held;

.5 areas where dangerous goods and hazardous substances are held;

.6 vessel traffic management system control rooms, aids to navigation and port control buildings, including security and surveillance control rooms;

.7 areas where security and surveillance equipment are stored or located;

.8 essential electrical, radio and telecommunication, water and other utility installations; and

.9 other locations in the port facility where access by vessels, vehicles and individuals should be restricted.

16.26 The security measures may extend, with the agreement of the relevant authorities, to restrictions on unauthorized access to structures from which the port facility can be observed.

Security level 1

16.27 At security level 1, the PFSP should establish the security measures to be applied to restricted areas, which may include:

.1 provision of permanent or temporary barriers to surround the restricted area, whose standard should be accepted by the Contracting Government;

.2 provision of access points where access can be controlled by security guards when in operation and which can be effectively locked or barred when not in use;

.3 providing passes which must be displayed to identify individual's entitlement to be within the restricted area;

.4 clearly marking vehicles allowed access to restricted areas;

.5 providing guards and patrols;

.6 providing automatic intrusion-detection devices, or surveillance equipment or systems to detect unauthorized access into, or movement within, restricted areas; and

.7 control of the movement of vessels in the vicinity of ships using the port facility.

Security level 2

16.28 At security level 2, the PFSP should establish the enhancement of the frequency and intensity of the monitoring of, and control of access to, restricted areas. The PFSP should establish the additional security measures, which may include:

.1 enhancing the effectiveness of the barriers or fencing surrounding restricted areas, including the use of patrols or automatic intrusion-detection devices;

.2 reducing the number of access points to restricted areas and enhancing the controls applied at the remaining accesses;

.3 restrictions on parking adjacent to berthed ships;

.4 further restricting access to the restricted areas and movements and storage within them;

.5 use of continuously monitored and recording surveillance equipment;

.6 enhancing the number and frequency of patrols, including water-side patrols, undertaken on the boundaries of the restricted areas and within the areas;

.7 establishing and restricting access to areas adjacent to the restricted areas; and

.8 enforcing restrictions on access by unauthorized craft to the waters adjacent to ships using the port facility.

Security level 3

16.29 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility in close co-operation with those responding and the ships at the port facility, which may include:

.1 setting up of additional restricted areas within the port facility in proximity to the security incident, or the believed location of the security threat, to which access is denied; and

.2 preparing for the searching of restricted areas as part of a search of all, or part, of the port facility.

Handling of cargo

16.30 The security measures relating to cargo handling should:

.1 prevent tampering; and

.2 prevent cargo that is not meant for carriage from being accepted and stored within the port facility.

16.31 The security measures should include inventory control procedures at access points to the port facility. Once within the port facility, cargo should be capable of being identified as having been checked and accepted for loading onto a ship or for temporary storage in a restricted area while awaiting loading. It may be appropriate to restrict the entry of cargo to the port facility that does not have a confirmed date for loading.

Security level 1

16.32 At security level 1, the PFSP should establish the security measures to be applied during cargo handling, which may include:

.1 routine checking of cargo, cargo transport units and cargo storage areas within the port facility prior to, and during, cargo handling operations;

.2 checks to ensure that cargo entering the port facility matches the delivery note or equivalent cargo documentation;

.3 searches of vehicles; and

.4 checking of seals and other methods used to prevent tampering upon entering the port facility and upon storage within the port facility.

16.33 Checking of cargo may be accomplished by some or all of the following means:

.1 visual and physical examination; and

.2 using scanning/detection equipment, mechanical devices, or dogs.

16.34 When there are regular or repeated cargo movements, the CSO or the SSO may, in consultation with the port facility, agree arrangements with shippers or others responsible for such cargo covering off-site checking, sealing, scheduling, supporting documentation, etc. Such arrangements should be communicated to and agreed with the PFSO concerned.

Security level 2

16.35 At security level 2, the PFSP should establish the additional security measures to be applied during cargo handling to enhance control, which may include:

.1 detailed checking of cargo, cargo transport units and cargo storage areas within the port facility;

.2 intensified checks, as appropriate, to ensure that only the documented cargo enters the port facility, is temporarily stored there and is then loaded onto the ship;

.3 intensified searches of vehicles; and

.4 increased frequency and detail in checking of seals and other methods used to prevent tampering.

16.36 Detailed checking of cargo may be accomplished by some or all of the following means:

.1 increasing the frequency and detail of checking of cargo, cargo transport units and cargo storage areas within the port facility (visual and physical examination);

.2 increasing the frequency of the use of scanning/detection equipment, mechanical devices, or dogs; and

.3 co-ordinating enhanced security measures with the shipper or other responsible party in addition to an established agreement and procedures.

Security level 3

16.37 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility in close co-operation with those responding and the ships at the port facility, which may include:

.1 restriction or suspension of cargo movements or operations within all, or part, of the port facility or specific ships; and

.2 verifying the inventory of dangerous goods and hazardous substances held within the port facility and their location.

Delivery of ship's stores

16.38 The security measures relating to the delivery of ship's stores should:

.1 ensure checking of ship's stores and package integrity;

.2 prevent ship's stores from being accepted without inspection;

.3 prevent tampering;

.4 prevent ship's stores from being accepted unless ordered;

.5 ensure searching the delivery vehicle; and

.6 ensure escorting delivery vehicles within the port facility.

16.39 For ships regularly using the port facility it may be appropriate to establish procedures involving the ship, its suppliers and the port facility covering notification and timing of deliveries and their documentation. There should always be some way of confirming that stores presented for delivery are accompanied by evidence that they have been ordered by the ship.

Security level 1

16.40 At security level 1, the PFSP should establish the security measures to be applied to control the delivery of ship's stores, which may include:

.1 checking of ship's stores;

.2 advance notification as to composition of load, driver details and vehicle registration; and

.3 searching the delivery vehicle.

16.41 Checking of ship's stores may be accomplished by some or all of the following means:

.1 visual and physical examination; and

.2 using scanning/detection equipment, mechanical devices or dogs.

Security level 2

16.42 At security level 2, the PFSP should establish the additional security measures to be applied to enhance the control of the delivery of ship's stores, which may include:

.1 detailed checking of ship's stores;

.2 detailed searches of the delivery vehicles;

.3 co-ordination with ship personnel to check the order against the delivery note prior to entry to the port facility; and

.4 escorting the delivery vehicle within the port facility.

16.43 Detailed checking of ship's stores may be accomplished by some or all of the following means:

.1 increasing the frequency and detail of searches of delivery vehicles;

.2 increasing the use of scanning/detection equipment, mechanical devices, or dogs; and

.3 restricting, or prohibiting, entry of stores that will not leave the port facility within a specified period.

Security level 3

16.44 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility, in close co-operation with those responding and the ships at the port facility, which may include preparation for restriction, or suspension, of the delivery of ship's stores within all, or part, of the port facility.

Handling unaccompanied baggage

16.45 The PFSP should establish the security measures to be applied to ensure that unaccompanied baggage (i.e. any baggage, including personal effects, which is not with the passenger or member of ship's personnel at the point of inspection or search) is identified and subjected to appropriate screening, including searching, before is allowed in the port facility and, depending on the storage arrangements, before it is transferred between the port facility and the ship. It is not envisaged that such baggage will be subjected to screening by both the port facility and the ship, and in cases where both are suitably equipped, the responsibility for screening should rest with the port facility. Close co-operation with the ship is essential and steps should be taken to ensure that unaccompanied baggage is handled securely after screening.

Security level 1

16.46 At security level 1, the PFSP should establish the security measures to be applied when handling unaccompanied baggage to ensure that unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

Security level 2

16.47 At security level 2, the PFSP should establish the additional security measures to be applied when handling unaccompanied baggage which should include 100 percent x-ray screening of all unaccompanied baggage.

Security level 3

16.48 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility in close co-operation with those responding and the ships at the port facility, which may include:

.1 subjecting such baggage to more extensive screening, for example x-raying it from at least two different angles;

.2 preparations for restriction or suspension of handling of unaccompanied baggage; and

.3 refusal to accept unaccompanied baggage into the port facility.

Monitoring the security of the port facility

16.49 The port facility security organization should have the capability to monitor the port facility and its nearby approaches, on land and water, at all times, including the night hours and periods of limited visibility, the restricted areas within the port facility, the ships at the port facility and areas surrounding ships. Such monitoring can include use of:

.1 lighting;

.2 security guards, including foot, vehicle and waterborne patrols; and

.3 automatic intrusion-detection devices and surveillance equipment.

16.50 When used, automatic intrusion-detection devices should activate an audible and/or visual alarm at a location that is continuously attended or monitored.

16.51 The PFSP should establish the procedures and equipment needed at each security level and the means of ensuring that monitoring equipment will be able to perform continually, including consideration of the possible effects of weather or of power disruptions.

Security level 1

16.52 At security level 1, the PFSP should establish the security measures to be applied, which may be a combination of lighting, security guards or use of security and surveillance equipment to allow port facility security personnel to:

.1 observe the general port facility area, including shore- and water-side accesses to it;

.2 observe access points, barriers and restricted areas; and

.3 allow port facility security personnel to monitor areas and movements adjacent to ships using the port facility, including augmentation of lighting provided by the ship itself.

Security level 2

16.53 At security level 2, the PFSP should establish the additional security measures to be applied to enhance the monitoring and surveillance capability, which may include:

.1 increasing the coverage and intensity of lighting and surveillance equipment, including the provision of additional lighting and surveillance coverage;

.2 increasing the frequency of foot, vehicle or waterborne patrols; and

.3 assigning additional security personnel to monitor and patrol.

Security level 3

16.54 At security level 3, the port facility should comply with the instructions issued by those responding to the security incident or threat thereof. The PFSP should detail the security measures which could be taken by the port facility in close co-operation with those responding and the ships at the port facility, which may include:

.1 switching on all lighting within, or illuminating the vicinity of, the port facility;

.2 switching on all surveillance equipment capable of recording activities within, or adjacent to, the port facility; and

.3 maximizing the length of time such surveillance equipment can continue to record.

Differing security levels

16.55 The PFSP should establish details of the procedures and security measures the port facility could adopt if the port facility is at a lower security level than that applying to a ship.

Activities not covered by the Code

16.56 The PFSP should establish details of the procedures and security measures the port facility should apply when:

.1 it is interfacing with a ship which has been at a port of a State which is not a Contracting Government;

.2 it is interfacing with a ship to which this Code does not apply; and

.3 it is interfacing with fixed or floating platforms or mobile offshore drilling units on location.

Declarations of Security

16.57 The PFSP should establish the procedures to be followed when, on the instructions of the Contracting Government, the PFSO requests a Declaration of Security (DoS) or when a DoS is requested by a ship.

Audit, review and amendment

16.58 The PFSP should establish how the PFSO intends to audit the continued effectiveness of the PFSP and the procedure to be followed to review, update or amend the PFSP.

16.59 The PFSP should be reviewed at the discretion of the PFSO. In addition it should be reviewed:

.1 if the PFSA relating to the port facility is altered;

.2 if an independent audit of the PFSP or the Contracting Government's testing of the port facility security organization identifies failings in the organization or questions the continuing relevance of significant elements of the approved PFSP;

.3 following security incidents or threats thereof involving the port facility; and

.4 following changes in ownership or operational control of the port facility.

16.60 The PFSO can recommend appropriate amendments to the approved plan following any review of the plan. Amendments to the PFSP relating to:

.1 proposed changes which could fundamentally alter the approach adopted to maintaining the security of the port facility; and

.2 the removal, alteration or replacement of permanent barriers, security and surveillance equipment and systems, etc., previously considered essential in maintaining the security of the port facility

should be submitted to the Contracting Government that approved the original PFSP for their consideration and approval. Such approval can be given by, or on behalf of, the Contracting Government with, or without, amendments to the proposed changes. On approval of the PFSP, the Contracting Government should indicate which procedural or physical alterations have to be submitted to it for approval.

Approval of port facility security plans

16.61 PFSPs have to be approved by the relevant Contracting Government, which should establish appropriate procedures to provide for:

.1 the submission of PFSPs to them;

.2 the consideration of PFSPs;

.3 the approval of PFSPs, with or without amendments;

.4 consideration of amendments submitted after approval; and

.5 procedures for inspecting or auditing the continuing relevance of the approved PFSP.

At all stages, steps should be taken to ensure that the contents of the PFSP remain confidential.

Statement of Compliance of a Port Facility

16.62 The Contracting Government within whose territory a port facility is located may issue an appropriate Statement of Compliance of a Port Facility (SoCPF) indicating:

.1 the port facility;

.2 that the port facility complies with the provisions of chapter XI-2 and part A of the Code;

.3 the period of validity of the SoCPF, which should be specified by the Contracting Governments but should not exceed five years; and

.4 the subsequent verification arrangements established by the Contracting Government and a confirmation when these are carried out.

16.63 The Statement of Compliance of a Port Facility should be in the form set out in the appendix to this Part of the Code. If the language used is not Spanish, French or English, the Contracting Government, if it considers it appropriate, may also include a translation into one of these languages.

17 PORT FACILITY SECURITY OFFICER

General

17.1 In those exceptional instances where the ship security officer has questions about the validity of identification documents of those seeking to board the ship for official purposes, the port facility security officer should assist.

17.2 The port facility security officer should not be responsible for routine confirmation of the identity of those seeking to board the ship.

In addition, other relevant guidance is provided under sections 15, 16 and 18.

18 TRAINING, DRILLS AND EXERCISES ON PORT FACILITY SECURITY

Training

18.1 The port facility security officer should have knowledge and receive training, in some or all of the following, as appropriate:

.1 security administration;

.2 relevant international conventions, codes and recommendations;

.3 relevant Government legislation and regulations;

.4 responsibilities and functions of other security organizations;

.5 methodology of port facility security assessment;

.6 methods of ship and port facility security surveys and inspections;

.7 ship and port operations and conditions;

.8 ship and port facility security measures;

.9 emergency preparedness and response and contingency planning;

.10 instruction techniques for security training and education, including security measures and procedures;

.11 handling sensitive security-related information and security-related communications;

.12 knowledge of current security threats and patterns;

.13 recognition and detection of weapons, dangerous substances and devices;

.14 recognition, on a non-discriminatory basis, of characteristics and behavioural patterns of persons who are likely to threaten the security;

.15 techniques used to circumvent security measures;

.16 security equipment and systems, and their operational limitations;

.17 methods of conducting audits, inspection, control and monitoring;

.18 methods of physical searches and non-intrusive inspections;

.19 security drills and exercises, including drills and exercises with ships; and

.20 assessment of security drills and exercises.

18.2 Port facility personnel having specific security duties should have knowledge and receive training in some or all of the following, as appropriate:

.1 knowledge of current security threats and patterns;

.2 recognition and detection of weapons, dangerous substances and devices;

.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten security;

.4 techniques used to circumvent security measures;

.5 crowd management and control techniques;

.6 security-related communications;

.7 operations of security equipment and systems;

.8 testing, calibration and maintenance of security equipment and systems;

.9 inspection, control, and monitoring techniques; and

.10 methods of physical searches of persons, personal effects, baggage, cargo, and ship's stores.

18.3 All other port facility personnel should have knowledge of and be familiar with relevant provisions of the port facility security plan in some or all of the following, as appropriate:

.1 the meaning and the consequential requirements of the different security levels;

.2 recognition and detection of weapons, dangerous substances and devices;

.3 recognition of characteristics and behavioural patterns of persons who are likely to threaten the security; and

.4 techniques used to circumvent security measures.

Drills and exercises

18.4 The objective of drills and exercises is to ensure that port facility personnel are proficient in all assigned security duties, at all security levels, and to identify any security-related deficiencies which need to be addressed.

18.5 To ensure the effective implementation of the provisions of the port facility security plan, drills should be conducted at least every three months unless the specific circumstances dictate otherwise. These drills should test individual elements of the plan such as those security threats listed in paragraph 15.11.

18.6 Various types of exercises, which may include participation of port facility security officers, in conjunction with relevant authorities of Contracting Governments, company security officers, or ship security officers, if available, should be carried out at least once each calendar year with no more than 18 months between the exercises. Requests for the participation of

company security officers or ship security officers in joint exercises should be made, bearing in mind the security and work implications for the ship. These exercises should test communication, co-ordination, resource availability and response. These exercises may be:

.1 full-scale or live;

.2 tabletop simulation or seminar; or

.3 combined with other exercises held, such as emergency response or other port State authority exercises.

19 VERIFICATION AND CERTIFICATION FOR SHIPS

No additional guidance.

APPENDIX TO PART B

APPENDIX 1

Form of a Declaration of Security between a ship and a port facility[2]

DECLARATION OF SECURITY

Name of ship:	
Port of registry:	
IMO Number:	
Name of port facility:	

This Declaration of Security is valid from ..... until ....., for the following activities:

.....
(list the activities with relevant details)

under the following security levels

Security level(s) for the ship:	
Security level(s) for the port facility:	

The port facility and ship agree to the following security measures and responsibilities to ensure compliance with the requirements of part A of the International Code for the Security of Ships and of Port Facilities.

	The affixing of the initials of the SSO or PFSO under these columns indicates that the activity will be done, in accordance with the relevant approved plan, by	
Activity	The port facility:	The ship:
Ensuring the performance of all security duties		
Monitoring restricted areas to ensure that only authorized personnel have access		
Controlling access to the port facility		
Controlling access to the ship		
Monitoring of the port facility, including berthing areas and areas surrounding the ship		
Monitoring of the ship, including berthing areas and areas surrounding the ship		
Handling of cargo		
Delivery of ship's stores		

[2] This form of Declaration of Security is for use between a ship and a port facility. If the Declaration of Security is to cover two ships, this model should be appropriately modified.

Handling unaccompanied baggage		
Controlling the embarkation of persons and their effects		
Ensuring that security communication is readily available between the ship and the port facility		

The signatories to this agreement certify that security measures and arrangements for both the port facility and the ship during the specified activities meet the provisions of chapter XI-2 and part A of the Code that will be implemented in accordance with the provisions already stipulated in their approved plan or the specific arrangements agreed to and set out in the attached annex.

Dated at .....on the .....

Signed for and on behalf of	
the port facility:	the ship:
(Signature of Port Facility Security Officer)	*(Signature of Master or Ship Security Officer)*

Name and title of person who signed	
Name:	Name:
Title:	Title:

Contact details *(to be completed as appropriate)* *(indicate the telephone numbers or the radio channels or frequencies to be used)*	
for the port facility:	for the ship:
Port facility	Master
Port facility security officer	Ship security officer
	Company
	Company security officer

APPENDIX 2

Form of a Statement of Compliance of a Port Facility

STATEMENT OF COMPLIANCE OF A PORT FACILITY

(Official seal) *(State)*

Statement Number .....

Issued under the provisions of part B of the INTERNATIONAL CODE FOR THE SECURITY OF SHIPS AND OF PORT FACILITIES (ISPS CODE)

The Government of_____
(name of the State)

Name of the port facility : .....
Address of the port facility : .....

THIS IS TO CERTIFY that the compliance of this port facility with the provisions of chapter XI-2 and part A of the International Code for the Security of Ships and of Port Facilities (ISPS Code) has been verified and that this port facility operates in accordance with the approved port facility security plan. This plan has been approved for the following <specify the types of operations, types of ship or activities or other relevant information> (delete as appropriate):

Passenger ship
Passenger high-speed craft
Cargo high-speed craft
Bulk carrier
Oil tanker
Chemical tanker
Gas carrier
Mobile offshore drilling units
Cargo ships other than those referred to above

This Statement of Compliance is valid until ....., subject to verifications (as indicated overleaf)

Issued at..... .....
(place of issue of the statement)

Date of issue..... .....
(Signature of the duly authorized official issuing the document)

(Seal or stamp of issuing authority, as appropriate)

ENDORSEMENT FOR VERIFICATIONS

The Government of <*insert name of the State*> has established that the validity of this Statement of Compliance is subject to <*insert relevant details of the verifications (e.g. mandatory annual or unscheduled)*>.

THIS IS TO CERTIFY that, during a verification carried out in accordance with paragraph B/16.62.4 of the ISPS Code, the port facility was found to comply with the relevant provisions of chapter XI-2 of the Convention and Part A of the ISPS Code.

1st VERIFICATION

Signed: .....
(Signature of authorized official)
Place: .....
Date: .....

2nd VERIFICATION

Signed: .....
(Signature of authorized official)
Place: .....
Date: .....

3rd VERIFICATION

Signed: .....
(Signature of authorized official)
Place: .....
Date: .....

4th VERIFICATION

Signed: .....
(Signature of authorized official)
Place: .....
Date: .....

第 23/2015 號行政長官公告

中華人民共和國於一九九九年十二月十三日以照會通知聯合國秘書長，經修訂的《1974年國際海上人命安全公約》自一九九九年十二月二十日起適用於澳門特別行政區；

國際海事組織海上安全委員會於二零零六年十二月八日透過第MSC.218（82）號決議通過了《國際救生設備規則》（《救生設備規則》）的修正案，有關修正案自二零零八年七月一日起適用於澳門特別行政區；

基於此，行政長官根據澳門特別行政區第3/1999號法律第六條第一款的規定，命令公佈包含上指修正案的第MSC.218（82）號決議的中文及英文文本。

二零一五年四月十四日發佈。

行政長官　崔世安

Aviso do Chefe do Executivo n.º 23/2015

Considerando que a República Popular da China, por nota datada de 13 de Dezembro de 1999, notificou o Secretário-Geral das Nações Unidas sobre a aplicação da Convenção Internacional para a Salvaguarda da Vida Humana no Mar de 1974, tal como emendada, na Região Administrativa Especial de Macau a partir de 20 de Dezembro de 1999;

Considerando igualmente que, em 8 de Dezembro de 2006, o Comité de Segurança Marítima da Organização Marítima Internacional, através da resolução MSC.218(82), adoptou emendas ao Código Internacional dos Meios de Salvação (Código LSA), e que tais emendas são aplicáveis na Região Administrativa Especial de Macau desde 1 de Julho de 2008;

O Chefe do Executivo manda publicar, nos termos do n.º 1 do artigo 6.º da Lei n.º 3/1999 da Região Administrativa Especial de Macau, a resolução MSC.218(82), que contém as referidas emendas, nos seus textos em línguas chinesa e inglesa.

Promulgado em 14 de Abril de 2015.

O Chefe do Executivo, *Chui Sai On*.