REPUBLIC OF MAURITIUS

Ministry of Public Infrastructure, Land Transport and Shipping
4th Floor, New Government Centre
PORT-LOUIS

MERCHANT SHIPPING NOTICE NO 3 OF 2004

Title: SHIP SECURITY GUIDELINES

The International Code for the Security of Ships and Port Facilities (ISPS Code)

Notice to*:* Mauritius Ports Authority, Owners/Operators, Charterers, Masters, Chief Engineers and Recognised Security Organisations

The **Director of Shipping** has developed the following Guidelines in compliance with the International Ship and Port Facility Security Code (ISPS) concerning ship security.

PREFACE:

1. The objective of these guidelines on Ship Security is to assist industry, employers, workers and others involved to respond to the risk to vessels from the threat posed by unlawful acts in the maritime environment. The guidelines provide guidance framework to develop and implement a ship security strategy commensurate with identified threats to security.

2. The Guidelines on ship security is part of an integrated approach to security and safety without prejudice to what is contemplated in the ISPS Code.

3. The International Maritime Organisation's (IMO) adoption in December 2002 of amendments to its SOLAS Convention and the ISPS Code addressed both ship and port facility (location where the ship/port interface takes place) security. These guidelines are intended to be compatible with the provisions of the **SOLAS ISPS Code**.

4. Ship security guidelines, as far as possible and except for ease of reference, should not replace, duplicate or create extraneous procedures or functions to those in the ISPS Code. Where there is no ISPS terminology, definition or procedure that meets the requirements of these guidelines alternative terminology, definitions and procedures should be compatible with the ISPS Code.

5. Nothing in these guidelines is intended to prejudice the rights or obligations of the State under international law. These guidelines should be interpreted in a manner that does not undermine the ILO conventions on workers rights.

6. These security guidelines do not override or abrogate the **Director of Shipping**, or any authorized in their behalf, as well as any commercial and industrial corporation or an individual's responsibility to comply with the laws, regulations and rules applicable in the respective port of the **Republic of Mauritius**. The guidance is not a substitute for applicable legal requirements nor is it regulation itself.

7. The scope of the guidelines is to promote recognized security roles, tasks and measures to deter, detect and respond to unlawful acts against vessels serving on international voyages and maritime operations.

8. These guidelines were developed to assist owners and operators to establish protective measures that are appropriate to their specific vessel.
Knowing that vessels are unique, owners and/or operators may seek an alternative to the specific protective measures recommended, demonstrating that such alternative to the protective measure provides an acceptable level of protection.

Director of Shipping
Ministry of Public Infrastructure,
Land Transport and Shipping
4th Floor, New Government Centre
Port Louis
Republic of Mauritius

ANNEX 'A'

SHIP SECURITY OFFICERS GUIDELINES

1. Section 12 of Part A of the ISPS Code requires that companies designate a Ship Security Officer (SSO) on each ship.

2. The duties and responsibilities of the SSO include, but are not limited to (Part A 12.2 ISPS Code):

    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 (SSP), monitoring the continuing relevance and effectiveness of the Plan, including the undertaking of internal audits and 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 (PFSO);

    4. Proposing modifications to the SSP;

    5. Reporting to the Company Security Officer (CSO) 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 SSP with the CSO and the relevant PFSO;

    10. Ensuring that any security equipment is properly operated, tested, calibrated and maintained;

    11. Reviewing and completing the Declaration of Security (DOS) on behalf of the ship.

3. According with Part B 13.1 ISPS Code requires the SSO to 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 SSA;

6. Methods of Ship Security Surveys and inspections;

7. Ship and port operations 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 weapons, dangerous substances and devices;

14. Recognition, on a non-discriminatory basis, of characteristics and behavioral patterns of persons who are like 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 the port facilities;

20. Assessment of security drills and exercises.

4. In addition the SSO should have adequate knowledge of, and receive training in, some or all of the following ship specific areas, as appropriate (Part B 13.2 ISPS Code):

    1. The layout of the ship;

    2. The SSP and related procedures (including scenario-based training on how to respond);

    3. Crowd management and control techniques;

    4. Operation of security equipment and systems;

5. Testing, calibration and, whilst at sea, maintenance of security equipment and systems.

5. Other shipboard personnel having specific security duties should have sufficient knowledge and ability to perform their assigned duties, including, as appropriate (Part B 13.3 ISPS Code):

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 behavioral patterns of persons who are like 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, whilst at sea, maintenance of security equipment and systems;

10. Inspection, control and monitoring techniques;

11. Methods of physical searches of persons, personal effects, baggage, cargo and ship’s stores.

6. All other shipboard personnel should have sufficient knowledge of and be familiar with relevant provisions of the SSP, including (Part B 13.4 ISPS Code)

    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 behavioral patterns of persons who are considered apt to threaten security;

    5. Techniques used to circumvent security measures.

ANNEX 'B'

SHIP SECURITY ASSESSMENT GUIDELINES

1. Section 8 of Part A of the ISPS Code requires the Company Security Officer (CSO) to ensure that, for each ship for which he has security responsibilities, a Security Assessment is carried out by persons with appropriate skills to evaluate the security of a ship, in accordance with ISPS Code.

2. The Ship Security Assessment (SSA) is considered to be an essential and integral part of the process of developing and updating the Ship Security Plan.

3. A Shipping Company can carry out its own SSA.

4. The SSA must 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.

    5. The SSA must be documented, reviewed, accepted and retained by the Company.

    6. 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 and specific guidance offered by the Contracting Governments.

    7. A SSA should address the following elements on board 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; &

6. other areas that may, if damaged or used for illicit observation, pose a risk to people, property, or operations on board the ship or within a port facility.

8. Those involved in a SSA should be able to draw upon expert in assistance regarding 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 characteristic and behavioral patterns persons who are likely to threaten security;

4. techniques used to circumvent security incident;

5. methods used to cause a security incident.

6. effects of explosives on ship 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.

9. 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 the bridge, spaces in which the main propulsion or generating machinery, navigation equipment, fire control station, emergency power and communications are located.

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. cargo spaces and stowage arrangements;

6. locations where the ship's stores and essential maintenance equipment is stores;

7. locations where unaccompanied baggage is stored;

8. emergency and stand-by equipment available to maintain essential services;

9. number of ship's personnel, any existing security duties and any existing training practices 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/waterside 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 communications, alarms, lighting, access control and other appropriate systems.

10. 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 relevant to:

1. restricted areas;

2. 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. access control systems, including identification systems;

6. security communications systems and procedures;

7. security doors, barriers and lighting; and

8. security and surveillance equipment and systems, if any

11. 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. ship's stores;

    6. any ship security communications equipment and systems; and

    7. any ship's security surveillance equipment and systems.

12. 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. ship's stores;

    6. any ship security communication equipment and systems; and

    7. any ship's security surveillance equipment and systems.

13. 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 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 used, 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.

14. 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, and any implications to crew fatigue, alertness and performance;

4. any identified security training deficiencies; and

5. any security equipment and systems, including communication systems.

15. T he 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.

16. Upon completion of the SSA, a report must 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 counter measures that could be used to address each vulnerability. The report must be protected from unauthorized access or disclosure.

On Scene Security Survey

17. 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.

ANNEX 'C'

SHIP SECURITY PLAN GUIDELINES

1. According with the Part A 9, ISPS Code requires each ship to carry on board a Ship Security Plan (SSP) approval by its flag state or by an organization recognized by it to carry out such approvals, known as a Recognized Security Organization (RSO).

2. The Company Security Officer (CSO) has the responsibility of ensuring that the plan is prepared and submitted for approval. The content of each individual SSP will vary depending on the particular ship it covers. The Ship Security Assessments (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.

3. All SSP have to make provision for the three, internationally adopted, Security Levels:

   A- Security Level 1, normal; the level at which ships and port facilities will normally operate;

   B- Security Level 2, heightened; the level applying for as long as there is a heightened risk of a security incident;

   C- Security Level 3, exceptional; the level applying for the period of time when there is a probable or imminent risk of a security incident.

4. The Plan must be written in the working language **and** in the English language. The Plan must address, at least, the following (Part A 9.4 ISPS Code):

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

   2. Identification of the restricted areas and measures for the prevention of unauthorized access;

   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 and updating of the Plan ;

12. Procedures for reporting security incidents;

13. Identification of the Ship Security Officer (SSO);

14. Identification of the CSO including 24-hour contact details;

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

16. Frequency of testing or calibration of security equipment provided on board, if any;

17. Identification of the locations where the ship security alert system activation points are provided (this information should be kept elsewhere on board in a document know to the master, the SSO and other shipboard personnel as decided by the Company);

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

5. The SSP must (Part B 9.2 ISPS Code):

1. Detail 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 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;

7. Detail reporting procedures to the **Director of Shipping**;

6. In addition, the SSP should establish the following, which relate to all Security Levels (Part B 9.7 ISPS Code);

1. Duties and responsibilities of all shipboard personnel with a security role;

2. Procedures of safeguards necessary to allow continuous communications to be maintained at all times;

3. 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 systems failure or malfunction;

4. 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. Procedures to ensure the timely submission, and assessment, 0of reports relating to possible breaches of security or security concerns;

7. Procedures to establish, maintain and update an inventory of any dangerous goods or hazardous substances carried on board, including their location.

7. The Plan can be kept in an electronic format. In such case, it must be protected by measures aimed at preventing unauthorized access, disclosure, deletion, destruction or amendment (Part A 9.6 ISPS Code).

8. The Plan should address the security measures to be taken at each Security Level covering:

1. Access to the ship by ship's personnel, passengers, visitors, etc;

2. Restricted areas of the ship;

3. Handling of cargo;

4. Delivery ship's stores

5. Handling unaccompanied baggage;

6. Monitoring the security of the ship.

ANNEX 'D'

COMPANY SECURITY OFFICERS GUIDELINES

1. Section 11 of Part A of the ISPS Code requires each shipping Company to designate a person to act as the Company Security Officer (CSO) for one or more ships, depending on the number or types of ships the Company operates, provided it is clearly identified for which ships the person is responsible.

2. A Company may, depending on the number or types of ships it operates, designate several persons as Company Security Officers, provided it is clearly identified for which ships each person is responsible.

3. In respect of such ships, the duties and responsibilities of the Company Security Officer (CSO) include, but are not limited to (Part A 11.2 ISPS Code):

    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 Assessment (SSA) is carried out;

    3. Ensuring the development, the submission for approval, and thereafter the implementation and maintenance of the Ship Security Plan (SSP) and its placement on board the appropriate ship;

    4. Monitoring the continuing relevance and effectiveness of the plan, ensuring that the Ship Security Plan (SSP) is modified, as appropriate, to correct deficiencies and satisfies 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 Flag State or the Recognized Security Organization (RSO);

    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 (SSO) and the relevant Port Facility Security Officers (PFSO);

    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 relevant ship-specific information accurately;

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

4. According with Part B 13.1 ISPS Code requires the Company Security Officer (CSO), and appropriate shore based Company personnel, to have knowledge of, and training in, some or all 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 (SSA);
6. Methods of Ship Security Surveys and inspection.
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 behavioral 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 exercise with port facilities; and
20. Assessment of security drills and exercises.

ANNEX 'E'

MEASURES AT DIFFERENT SECURITY LEVELS

Measures which might be taken at each of the Security Levels outlined by the ISPS Code:

Security Level 1

For Access Control

1. The Ship Security Plan should establish the security measures to control access to the ship, where the following may be applied:

    1. checking the identify 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, ensuring that designated secure areas are established in which inspections and searching of people, baggage (including carry on items), personal effects, vehicles and their contents can take place;

    3. in liaison with the port facility, ensuring 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 Ship Security Plan.

    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.

Security Level 1
For Restricted Areas

1. The Ship Security Plan 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 1
For Handling of Cargo

2. The Ship Security Plan should establish the security measures to be applied during cargo handling, which may include.

    1. routine checking of cargo, cargo transport until 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 Ship Security Plan, and

    4. checking of seals or others methods used to prevent tampering.

Security Level 1
For Delivery of Ship's Stores

3. The Ship Security Plan 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 1
For Handling Unaccompanied Baggage

4. The Ship Security Plan should establish the security measures to be applied when handling unaccompanied baggage is screened or searched up to and including 100 percent, which may include use of x-ray screening.

Security Level 1

For Monitoring the Security of the Ship

5. The Ship Security Plan 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.

6. 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 underway, when necessary, ships should use the maximum lighting available consistent with safe navigation, having regard to the provisions of the **International Regulation for the Prevention of Collisions at Sea** in force.

7. The following should be considered when establishing the appropriate level and location of lighting:

    1. whilst at anchor or alongside, the ship's personnel should be able to detect activities beyond the ship, on both the shoreside and the waterside;

    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
For Access Control

1. The Ship Security Plan 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, the provision of boat
patrols in liaison with the port facility;

4. establishing a restricted area on the shoreside of the ship, in close co-operation with the port facility;

5. increasing the frequency and detail of searches of people, 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,

8. carrying out a full or partial search of the ship.

Security Level 2

Restricted Areas

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 Ship Security Plan 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 2

For Handling of Cargo

3. The Ship Security Plan 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.

4. 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-coordinating enhanced security measures with the shipper or other responsible party in accordance with an established agreement and procedures.

Security Level 2
For Delivery of Ship's Stores

5. The Ship Security Plan 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 2

For Handling Unaccompanied Baggage

6. The Ship Security Plan 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 2
For Monitoring the Security of the Ship

7. The Ship Security Plan 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 lookouts; and

4. ensuring co-ordination with waterside boat patrols, and foot or vehicle patrols on the shoreside, when provided.

Security Level 3

For Access Control

1. The Ship should comply with the instructions issued by those responding to the security incident or threat thereof. The Ship Security Plan 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. suspending embarkation or disembarkation;

    5. suspending cargo handling operations, deliveries etc;

    6. evacuating the ship;

    7. moving the ship; and

    8. preparing for a full or partial search of the ship.

Security Level 3

For Restricted Areas

2. The ship should comply with the instructions issued by those responding to the security incident or threat thereof. The Ship Security Plan 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. establishing 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 restricted areas as part of a search of the ship.

Security Level 3
For Handling of Cargo

3. The Ship should comply with the instructions issued by those responding to the security Incident or threat thereof. The Ship Security Plan 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 loading or unloading of cargo; and

    2. verifying the inventory of dangerous goods and hazardous substances carried on board, if any, and their location.

Security Level 3

For Delivery of Ship's Stores

1. The ship should comply with the instructions issued by those responding to the security Incident or threat thereof. The Ship Security Plan 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' stores on board the ship.

Security Level 3
For Handling Unaccompanied Baggage

2. The ship should comply with the instructions issued by those responding to the security incident or threat thereof. The Ship Security Plan 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. preparing to restrict or suspend the handling of unaccompanied baggage; and

    3. refusing to accept unaccompanied baggage on board the ship.

Security Level 3
For Monitoring the Security of the Ship

1. The Ship should comply with the instructions issued by those responding to the security incident or threat thereof. The Ship Security Plan 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 all lighting on the ship or illuminating its vicinity;

    2. switching on 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. preparing for underwater inspection of the hull of the ship; and

    5. initiating measures, including the slow revolution of the ship's propellers, if practicable, to deter underwater access to the hull of the ship.