



NATIONAL INTELLIGENCE AGENCY  
REPUBLIC OF SOUTH AFRICA

# **GUIDE TO PREPARING SECTION 5 OF A MARITIME SECURITY PLAN (PORT AND PORT FACILITIES)**

## **SECURITY MEASURES AND PROCEDURES FOR DIFFERENT MARITIME SECURITY LEVELS**



**IMPORTANT NOTE: GUIDE TO PREPARING SECTION 5 OF A MARITIME SECURITY PLAN (PORT AND PORT FACILITIES).**

1. This guide has been prepared in accordance with the *Merchant Shipping Act, 1951, Act 57 of 1951* (hereafter referred to as “the Act”) and the *Merchant Shipping (Maritime Security) Regulations, 2004* (hereafter referred to as “the Regulations”). The guide has been prepared by the National Intelligence Agency on request of the Maritime Security Advisory Committee (an inter-departmental committee that has been established to ensure compliance with the ISPS code by 1 July 2004). All care has been taken to ensure that this guide accurately reflects the requirements of the Act and Regulations.
2. The guide must be utilized as a template by Port and Port Facility Operators to prepare Section 5 of their Maritime Security Plan (the section that deals with Security Measures and Procedures to be implemented at the Port or Port Facility at the different Maritime Security Levels).
3. To ease the utilization of the template, Port and Port Facility Operators is advised to merely refer to attachment 4 in Section 5 of their plan, which will deal with the specific Security Measures and Procedures at the Port or Port Facility. The template has been designed that it can easily be pasted into any plan at Attachment 4 (after it has been adapted for a specific Port or Port Facility).
4. For further advice on utilizing the template, the following Counter Intelligence Advisors of the National Intelligence Agency (NIA) can be contacted:

Ms MG VAN DER MERWE

Tel : (012) 427-4158

Cell : 082 335 2485

Mr G MULDER

Tel : (012) 427-5071

Cell : 082 335 2486

---

**EXAMPLE OF SECURITY MEASURES AND PROCEDURES AT THE DIFFERENT MARITIME SECURITY LEVELS TO BE INDICATED IN SECTION 5 OF THE GUIDE TO PREPARING A MARITIME SECURITY PLAN (PORTS AND PORT FACILITIES). THE ACTUAL EXAMPLE IS INTENDED FOR USE IN A TYPICAL PORT FACILITY SECURITY PLAN (PFSP) BUT CAN BE EASILY ADDAPTED FOR A PORT SECURITY PLAN (PSP).**

---

1. The following instructions are based on Marine Security Levels as defined in the Regulations. There are 3 levels of security depending on the potential of terrorist or other threat of unlawful activity at the port or port facility.
  - **MARITIME SECURITY LEVEL 1** – normal operating conditions, threat of unlawful act is possible but not likely.
  - **MARITIME SECURITY LEVEL 2** – threat of unlawful act is possible and intelligence indicates that terrorists are likely to be active within a specific area or against a type of vessel or Terminal.
  - **MARITIME SECURITY LEVEL 3** – threat of unlawful act is probable or imminent and intelligence indicates that terrorists have chosen specific targets.
2. **The DG will communicate the Maritime Security Level currently in effect to Port Operators and Port Facility Operators. All personnel working at the Port (or Port Facility), as well as personnel of Port Service Providers, shall be aware of the Maritime Security Level in effect and shall be familiar with the sections of this SECURITY PLAN related to the Maritime Security Level in effect, as outlined below.**
3. **DEFINITIONS**
  - 3.1 The following definitions are relevant to the understanding of the security instructions/measures in this section:
    - Terminal Area – That area, including all buildings, sheds, storage, tank farms, roadways and parking lots enclosed by the perimeter fencing.
    - Industrial Area – That area outside the Terminal building and terminal parking lot, but including the remainder of the Terminal Area.

---

**Attachment 4 - Security Measures and Procedures**

---

**MARITIME SECURITY LEVEL I – NORMAL OPERATING  
CONDITIONS**

**1. PHYSICAL SECURITY**

1.1 **South African Police Service (SAPS) Response.** Port/Port Facility security personnel are not armed. The local SAPS is available by calling Tel. Nr. .... for incidents of an emergency nature. The SAPS response time is **30 minutes** for non-emergency issues. For response to waterborne security threats, breaches or incidents, the following components of the SAPS and the Navy should be contacted:

.....

.....

**1.2 Restricted Areas**

1.2.1 The following areas in the main office building are restricted and locked at all times:

- Network file server room
- Office furnace room
- Office records archive room
- Electrical Room

1.2.2 The following areas in the Industrial Area are restricted and are to be locked at all times:

- Terminal Electrical Substation
- Pump Room
- Tank Farm

**1.3 Barriers and Gates**

1.3.1 Perimeter areas shall be clear of vegetation and debris that could obscure clear observation and which could be used to breach fences.

- 1.3.2 Water access is periodically patrolled by Port Authority or police craft.
- 1.3.3 Access gates shall be closed and locked during non-working hours and when not in use or under control of security officers or security staff.

#### **1.4 Fencing**

- 1.4.1 Perimeter fences are constructed of steel palisade and 2,5m high, including a 500mm anti-scaling extension above the fence. In some locations the fence is 4m high.
- 1.4.2 Perimeter gates are constructed of the same material.
- 1.4.3 Fence bottoms are secured in a 500mm concrete plinth that runs underneath the fence.
- 1.4.4 Security fences are to be kept clear of all obstructions.
- 1.4.5 Shift foremen are responsible to check fencing in their work area and report any breaches or damage to fencing to the PFSO when observed.

#### **1.5 Lighting.**

- 1.5.1 During night operations, all yard and stringer lights are on providing sufficient illumination in conformance with safety regulations. During night time non-operating hours, one light on each pole is left on providing a minimum of 1 foot-candle illumination in all Terminal locations. Lighting is directed downward, away from guards or offices, or navigable waterways and produces high contrast with few shadows.

## **2. SECURITY ALARMS/VIDEO SURVEILLANCE/COMMUNICATION SYSTEMS**

### **2.1 Alarms**

- 2.1.1 The Terminal has an Emergency Siren alarm that is used for emergencies. On hearing the alarm all work is to stop and terminal workers are to follow the instructions announced over the loudspeaker public address system.

### **2.2 Video Surveillance**

- 2.2.1 The Terminal is equipped with video surveillance cameras on the security office roof, terminal office roof and on sheds 1, 3, 5 and 7.

These cameras can be operated remotely from the security office to scan the roadways, perimeter fencing and to seaward along the pier wall. They are monitored by security officers 24 hours a day.

### **2.3 Communications Systems.**

- 2.3.1 Security communications are tested once each shift and recorded in the security log book.
- 2.3.2 Security officers to contact police or emergency response services in the event assistance is required; inform the Main Gate/Port Security Office in such an event.
- 2.3.3 Hand-held VHF radios carried by security officers are battery powered. A sufficient supply of charged batteries is maintained in event of power failure.
- 2.3.3 The phones at the main gate and VHF radios carried by security officers provide a dedicated communications system for the security component.
- 2.3.4 All security officers receive training in the Terminal Security Procedures, which includes instruction on use of the communications system.

## **3. SECURITY PATROLS AND INSPECTIONS**

- 3.1 Security officers shall conduct roving safety and security patrols of all areas of the Terminal including the areas of waterside access. Patrol vehicle mileage per shift shall be 10 to 20 km with odometer readings recorded each shift.
- 3.2 Security officers shall conduct rounds at least once in a four-hour period at varying times to prevent predictability. Particular attention shall be paid to all restricted areas and buildings.
- 3.3 The security officer at the Main Gate shall record the rounds conducted in the Main Gate Log Book, which is available for inspection by the PSO, PFSO, Duty Manager, Management and NIA Security Advisors.

## **4. REPORTING SECURITY INCIDENTS AND BREACHES OF SECURITY**

- 4.1 The primary function of roving security is detection and reporting of any incidents or breaches of security, which are to be reported immediately

to the PSO and the PFSO. The PFSO will inform Management and direct any additional calls to be made to SAPS, NIA or emergency services, as appropriate.

4.2 Security Incidents and Breaches of Security to be reported include:

- Unauthorized personnel gaining access to the Terminal.
- Unauthorized or improperly parked vehicles at the Terminal.
- Unauthorized vessel moored at the Terminal.
- Bomb threat.
- Suspicious persons or activity in or in the immediate vicinity of the Terminal.
- Loss of electrical power.
- Discovery of unknown/suspicious package at the Terminal.
- Breach of perimeter fence.
- Evidence of tampering with equipment, security systems, doors, windows, locks or other access points on any Terminal buildings.
- Compromise of sensitive/classified information.
- Compromise of IT and communication systems.

4.3 Additional details on handling each of the above incidents or breaches of security are covered later in this Plan.

**5. KEY/ID/ACCESS CARD CONTROL**

5.1 The security officers on duty at the Main Gate/Security Office or the PFSO are the only persons authorized to issue keys for specific areas of the Terminal. A log entry shall be made in the Key Register for the signing out and receipt of all keys, listing the person signing in/out, the date and time of the occurrence. Employees must show their issued photo ID prior to issue of keys. If they do not have a photo ID, they must show another valid photo ID which security will verify against the list of Employees.

5.2 The Main Gate/Security Office door shall be locked at all times and access provided only to on-duty security staff.

- 5.3 Locks are inspected regularly and malfunctioning locks are replaced if found in bad order. The same applies for locks of which the keys has been lost.
- 5.4 Only case hardened security locks are used and chains, where used, are permanently attached to gates.
- 5.5 Formal guidelines for computer security are available in the IT security policy of the port/port facility.
- 5.6 Access to computerized information is password protected and restricted on a need-to know basis according to job function. File servers are in a locked room. The Terminal's information systems provider, SITA, provides support, security and data integrity for all computer systems.
- 5.7 Terminal equipment is to be kept inside the locked perimeter fence to avoid access or tampering by unauthorized personnel. The prescribed control voucher must be utilized in the prescribed manner (signed by management to authorise the removal and presented to security at the main gate) in the event that equipment must be removed from the premises.

## 6. **TERMINAL AREA ACCESS CONTROL**

### 6.1 **Gates**

- 6.1.1 The main gate shall be locked during silent hours and monitored at all times. The longshoremen's parking lot gate shall be locked at all times except when a vessel is working. Other perimeter gates shall be locked at all times and monitored by video surveillance at the Main Gate/Security Office.

### 6.2 **Deliveries (of supplies and services)**

- 6.2.1 All packages entering or leaving the Terminal are subject to search by security officers, PFSO, Duty Manager or the SAPS. Signs are posted advising of this requirement at principal Terminal entry gates.

### 6.3 **Mail**

- 6.3.1 Normal mail is delivered to the Administration Office in the Terminal Building. Administration staff will make arrangements for pick up/delivery of oversized packages. Mail delivered by Courier Services

will be signed for at the Main Gate/Security Office by the security officers and delivered to the Administration Office.

#### **6.4 Deliveries**

6.4.1 Deliveries shall be scheduled in advance. Where not scheduled in advance, deliveries are prohibited until approved by the Duty Manager. The Duty Manager will provide a list to the Main Gate/Security Office of regularly authorized delivery companies having permission to bring vehicles onto the Terminal premises.

#### **6.5 Hazardous materials**

6.5.1 Hazardous materials shall not be permitted to enter the terminal area without verification by the PFSO or Duty Manager that the materials are expected for delivery and that safety and security precautions are in place prior to their acceptance. Precautions include transportation in properly marked vehicles and proper secure storage, availability of first aid fire fighting equipment and appropriate cleanup equipment.

#### **6.6 Vessel Arrival and Security Procedures While Moored.**

6.6.1 Unscheduled tugs, barges or other vessels are not permitted to berth alongside without prior notification from the Harbourmaster's office and notification of arrival to the PFSO, who will clear the arrival with management as required. Arriving vessel crews shall be advised of the applicable Maritime Security Level (1, 2 or 3).

6.6.2 Vessel crew may not exit or enter the Terminal without showing photo ID to the on watch Security Staff who shall verify their ID against the crew list.

6.6.3 Vessel agents shall whenever possible schedule deliveries of ships' stores in advance.

6.6.4 Vessels shall be advised of the phone number for Terminal security as well as the office and cell numbers for Terminal Management.

### **7. IDENTIFICATION PROCEDURES**

#### **7.1 Identification of Personnel Entering Terminal**

7.1.1 All personnel entering the Terminal area must present their Access Control Card at the Main Gate/Security Office to gain access. Individuals arriving by motorcycle shall remove helmets to assist in

identification. Security officers shall verify that ID matches the person presenting it.

- 7.1.2 While in the Terminal Area, all personnel must carry their Access Control Cards visibly displayed, and which must also be presented upon request of security officers, Duty Manager, PFSO or PSO. While conducting roving patrols, security officers or other competent authority shall challenge unknown or suspicious personnel to identify themselves with a valid issued access card. If the security officer does not know that the person has valid business at the Terminal, he shall contact the PFSO for authorization prior to allowing the person to enter.

## **7.2 Vendors/Contractors/Vessel Pilots/Agents**

- 7.2.1 Vendors, contractors, vessel pilots and agents must show valid photo ID prior to entry. Vendors, contractors, pilots, and agents should be scheduled in advance. The Duty Manager will provide the schedule to security staff. The Duty Manager will provide a list to the guard of pre-authorized, regularly scheduled vendors. Non-scheduled visits must be cleared with Terminal Management prior to entry. Vehicle Control Procedures (see below) apply if private vehicles are driven into the Terminal. Fast food deliveries are not permitted to enter the Terminal. Prior arrangements must be made to pick up and drop off such items at the Main Gate.

## **7.3 Port Authority Staff**

- 7.3.1 Port Authority employees entering the main gate with private vehicles or Port Authority vehicles must show valid photo ID prior to entry. Vehicle Control Procedures (see below) apply if private vehicles are driven into the Terminal.

## **7.4 Truck Drivers**

- 7.4.1 All truck drivers must show valid photo ID prior to entry. The Main Gate security officer will verify that drivers have valid business at the Terminal (for example, checking booking or bill of lading number). Passengers are not permitted in trucks unless authorized by Terminal Management.

## **7.5 Visitors**

- 7.5.1 All visitors must show valid photo ID prior to entry. Visitors are not authorized in the Industrial Area without a Terminal employee escort. Vehicle Control Procedures (see below) apply if private vehicles must be driven into the Terminal. Whenever possible, visitors shall be

scheduled in advance. If not, entry is not permitted until authorized by Terminal Management. This will ensure that visitors have valid business at the Terminal. Only visitors with official business at the Terminal will be allowed.

## 7.6 Government Employees

7.6.1 All government employees may enter the Terminal to conduct official business and must show valid government organization photo ID prior to entry. Security will direct government employees where to park vehicles.

## 7.7 Vessel Crew and Passengers.

7.7.1 The Crew List and Passenger List (if applicable) provided by the vessel in its pre-arrival notice report will be received by the PFSO from the Harbour Master. The PFSO will provide this list to the Main Gate/Security Office.

7.7.2 Crew and passengers who exit the gate cannot re-enter unless they show a photo ID which the security officer checks against the Crew List and Passenger List.

7.7.3 Unless instructed otherwise by government authority, crew and passengers may depart the vessel and proceed directly to their destination so as to avoid handling areas in the yard.

7.7.4 Crew and passenger vehicles are not permitted to enter the Terminal unless authorized by Terminal Management.

7.7.5 Passengers shall, if possible, be transported to and from the vessel with yard transport vehicles.

7.7.6 Taxis are not normally permitted to enter the Terminal, except in special circumstances, pre-arranged with the Main Gate/ Security Office and cleared by the PFSO.

## 7.8 Vehicle and Personnel Searches

7.8.1 All persons, packages and vehicles entering or leaving the Terminal are subject to search by security, Terminal Management or government authority.

7.8.2 Random inspections must be conducted on at least 5% of those entering the Terminal while the Terminal is at **Maritime Security Level 1**. This excludes freight containers.

## **7.9 Acceptable Identification in lieu of Port Access Control Card**

7.9.1 ID cards shall be tamper-resistant and laminated with photograph. ID cards shall show the relevant details of the holder, e.g., name, description or other pertinent data and are to be issued by a Government Institution. Acceptable identification includes:

- Valid driver's license.
- Photo ID card issued by a government institution (e.g. SAPS, SANDF or NIA appointment certificates/cards).
- Passport.
- Employee Photo ID from another Facility/Terminal at the port.
- SA ID book/card.

## **8. VEHICLE CONTROL/SECURITY**

### **8.1 Control of Motor Vehicles and Supplier/Contractor Vehicles**

8.1.1 Control of all motor and supplier/contractor vehicles is as specified below in "VEHICLE CONTROL PROCEDURES." Designated parking for employees is located outside the Terminal Area, adjacent to the fence next to the Terminal Building and next to the fence behind Sheds 2 and 4.

8.1.2 Vehicle entry at the Main Gate into the Terminal Area is limited to Management, Port Authority, Government Employees on official business and pre-approved suppliers/contractors when approved by Terminal Management. All vehicles entering or leaving the Main Gate are subject to search. Signs are posted at the main gate advising of this requirement.

8.1.3 Parking for vehicles authorized to enter the Terminal Area is restricted to specific areas. Parking in the Industrial Area is restricted to the parking lot to the east of the Terminal Building. Vehicles non-essential within the Terminal shall park in the fenced long shore parking lot, which is outside the Terminal Area.

## **9. VEHICLE CONTROL PROCEDURES**

9.1 Private vehicles that must enter the Terminal must be registered at the Main Gate. A Permanent Vehicle Pass will be issued for Management,

Port Authority, approved government vehicles and identified Supplier/Contractors' vehicles (on approval of the PFSO).

- 9.2 A Temporary Vehicle Pass (which must be displayed prominently in the vehicle front window) will be issued for all other vehicles authorized temporary access. Main Gate Security officers will instruct drivers where to park and the safest traffic pattern to follow depending on the type of operation in progress (container yard operation, container vessel, break-bulk vessel, etc.). Once the person has completed his or her visit, they will turn in their Temporary Vehicle Pass and the security officer will record the exit time. Government vehicles that have regular business at the terminal and clearly marked Port Authority vehicles are not required to be issued a Temporary Vehicle Pass.

## 10. RAIL SECURITY

- 10.1 Not applicable. Terminal does not currently have rail access.

**NOTE:** This is given as an example only in the event that one of the measures contained in this document are not applicable to a specific port facility. If the terminal does have rail access, security control measures must be mentioned here. The measures would be similar to those for controlling motor vehicle access.

## 11. CARGO SECURITY

- 11.1 All cargo/ships' stores awaiting a vessel's arrival shall be stored in Terminal Sheds and kept under lock and key until embarkation.
- 11.2 Security patrols shall also be regularly conducted in cargo storage areas.

## 12. WATERSIDE SECURITY

- 12.1 Waterside security is the responsibility of the local SAPS Water Wing. All personnel are to be vigilant when working in the docks areas and report any suspicious activity or security threats on the water or shorelines adjacent to the Terminal Area to the Main Gate/Security Office. Security officers are to further the report to the PFSO for action.

**13. TRAINING AND SECURITY AWARENESS**

- 13.1 All security officers must complete Security Awareness Training. In addition, security officers must complete a training program designed by the PFSO specific to the security requirements of the Terminal. The PFSO will maintain files on these training records in the Terminal office.
- 13.2 The Terminal security training program includes the following elements.
- Law enforcement and security guidelines.
  - Applicable security related legislation.
  - Minimum Information Security Standards.
  - Company policies including the security plan and response procedures.
  - Prevention, detection and investigation of criminal activities.
  - Reporting of threats or actual criminal and terrorist activity.
  - Operations of communications systems.
  - Procedures for notifying all Terminal personnel when higher security levels are imposed.
- 13.3 Security officers will be given an annual security awareness training refresher to ensure that they have an up-to-date working knowledge of the following:
- Port Security Plan.
  - Terminal Security Plan.
  - Terminal Emergency Response Plan.
  - Procedures for notifying police agencies.
  - Bomb Threat and other Emergency and Security Response Procedures.
- 13.4 The security officers training program is reviewed annually by the PFSO and security officers are re-certified annually. Once notified of an increase to a higher security level, the PFSO will inform all Security staff and security officers, as well as other management.

13.5 In addition to the above, all Terminal personnel must also complete a Security Awareness Training Program. The program will be designed and implemented by the PFSO. The essential elements of the Security Awareness Program for employees are:

- Port Security Plan.
- Terminal Security Plan.
- Terminal Emergency Response Plan.
- Procedures for notifying police agencies.
- Bomb Threat and other Emergency and Security Response Procedures.
- Minimum Information Security Standards.

13.5 The aim of the Security Awareness Program for employees is to ensure that all employees have an up-to-date working knowledge of the above as well as knowledge of their overall security responsibilities. The program must also be repeated annually.

#### 14. DRILLS AND EXERCISES

14.1 The PFSO is responsible for the scheduling and conduct of security drills and exercises, keeping management informed of when such events have been scheduled. Wherever possible, drills and exercises should include participation of any ships alongside, unless they decline. Drills shall be conducted at least quarterly. Exercises shall be conducted annually and if at all possible, in conjunction with exercises scheduled by the Port Authority.

#### 15. SECURITY RELATED RECORDS

15.1 Records may be kept in digital as well as paper format. All records shall be kept in secure storage. The PFSO is responsible for keeping the following records for a minimum of two years:

- The **Port Facility Security Assessment** and **Security Plan** that are in effect, any temporary or permanent amendments or additions and related Statements of Compliance;
- **Security training** and **Security Awareness Programs**, including the date, duration and description and names of the participants;

- **Security drills and exercises**, including the date, duration and description and names of the participants and any best practices or lessons learned;
- **Security incidents or breaches**, including the date, time, location and description and to whom it was reported;
- **Changes in Maritime Security Levels**, including the date, time of notification received and time of compliance with the requirements of that level, in accordance with this plan;
- **Maintenance, calibration, and testing of security equipment;**
- **Security threats** including the date, time and manner of communication, who received or identified the threat and a description of the threat and the response;
- **Security threats of a terrorist nature**, including the date, time, description of the threat, who received or identified the threat and measures taken to prevent or protect from attack; and
- A copy of every single **visit declaration of security** and a copy of every continuing declaration of security for at least 90 days after its effective period.

## 16. **RESPONSE PROCEDURES**

- 16.1 If a security incident or breach of security should occur, it should be reported to the Security officers at the Main Gate/Security Office who shall report the incident or breach by calling the Port Authority Security Component/PSO and the PFSO from the SECURITY AND EMERGENCY CONTACT LIST. The PFSO will direct any additional calls to be made from the other numbers on the list. The PFSO will ensure that Security Incidents and breaches of security are reported to the relevant authorities (e.g. NIA, SAPS, SANDF, NDOT) as soon as possible.

### 16.2 **Evacuation for Security Incident**

16.2.1 Any evacuation of the Terminal Area shall be executed only on order of the PFSO and shall be supervised by Security officers. Notice of the requirement to evacuate will be given over the loudspeaker system following activation of the Emergency Siren. The Gathering Area for all Terminal Employees and Longshoremen is the Parking Lot outside the Terminal Area.

**16.3 Unauthorized personnel or vehicle discovered in the Terminal Area**

- Ensure that the Port Authority and the PFSO is notified. Attempt to determine person's identity/vehicle ownership and why they are in the Terminal Area.
- The PFSO, if necessary, will call the local police. If for some reason the PFSO is unavailable, the Security officer on duty shall call the local police.
- The security officers will monitor the unauthorized person/vehicle until police arrives.
- Notify NIA, NDOT or SANDF as necessary.

**16.4 Unauthorized vessel moored at the Terminal**

- Ensure the Harbourmaster/Port Authority and the PFSO is notified.
- Inform Duty Manager as directed by PFSO.
- Security officers will monitor the unauthorized vessel until police arrives.
- Security officers to photograph the vessel including Registry numbers if possible.
- Notify NIA, NDOT or SANDF as necessary.

**16.5 Bomb Threat – See Annex A.**

**16.6 Suspicious person(s) or activity.**

**<CONFIDENTIAL WHEN COMPLETED>**

- Security officers shall notify PFSO, who will direct next actions to be taken.
- If directed by PFSO, local police and Port Authority must be notified.
- If directed by PFSO, prepare to direct police to search the area and arrest the individual(s)
- Obtain photograph(s) if able to do so without risk.
- Notify NIA, NDOT or SANDF as necessary.

**16.7 Loss of Power/Lighting**

- Security officers shall notify Duty Manager.
- Utilizing emergency lights/available flashlights, truck headlights, etc., evacuate personnel to safe areas (roadways/parking lot).
- Ensure all gates and offices are locked.
- Duty Manager/Terminal Management will notify Harbourmaster/Port Authority.

**16.8 Receipt of Suspicious Mail or Package**

- Call the Main Gate/Security Office. A security officer will attend the office or location of the suspicious mail/package and evacuate the area/isolate the mail/package.
- Security officer shall notify the PFSO, who will direct next actions to be taken.
- If directed by PFSO, notify local police, Port Authority and Harbourmaster.
- If directed by PFSO, prepare to direct police to site of suspicious mail/package.
- Obtain photograph(s) if able to do so without risk.
- Notify NIA, NDOT or SANDF as necessary.

## MARITIME SECURITY LEVEL 2 – INCREASED ALERT

**Additional Measures for Maritime Security Level 2 condition: threat of unlawful act is possible and intelligence indicates that terrorists are likely to be active within a specific area or against a type of vessel or Terminal.**

### 1. GENERAL

- 1.1 The Terminal Manager, Duty Manager, PFSO or other appointed personnel with access to building plans as well as the plans for area evacuations must be available at all times. All security plans, orders, personnel details and logistic requirements related to the implementation of **Maritime Security Level 2** shall be reviewed to confirm they are up to date.
- 1.2 Terminal personnel are to be made aware of the general situation in order to stop rumours and prevent unnecessary alarm. All personnel should be aware that **Maritime Security Level 2** is in force and all should be advised to be extra vigilant in their day to day work.

### 2. PHYSICAL SECURITY

- 2.1 Security officers shall increase frequency of rounds and random checks of restricted areas, waterfront areas, the main pier, vehicles, Terminal buildings and sheds and other areas of risk or vulnerability.
- 2.2 At the beginning and end of each workday, as well as at other regular and frequent intervals, inspect the interior and exterior of buildings in regular use for suspicious packages.
- 2.3 Security officers will report to management on the current security situation at the Port Facility at least once every 4 hours.
- 2.4 All Mail shall be carefully examined by Main Gate/Security Office security officers prior to being delivered to other offices in the Terminal Buildings paying particular attention for letter or parcel bombs.
- 2.5 Where possible such objects as crates, garbage containers, etc are to be moved at least 50 metres from the Terminal buildings, the Main Gate/Security Office, warehouses and sheds.

**3. LIGHTING**

- 3.1 All Terminal Building, industrial area, tank farm, warehouse and stringer lights will be on at night.

**4. COMMUNICATION SYSTEMS**

- 4.1 Telephones and radios shall be tested by security officers at every change of watch and at increase of security level.

**5. ACCESS CONTROLS**

- 5.1 All visitors, contractors, vendors and other Terminal guests shall be escorted to and from their destination. The escort may be a security officer or a terminal employee.
- 5.2 All passenger/crew baggage must be X-Rayed.
- 5.3 All passenger/crew baggage must be screening for explosives.
- 5.4 All deliveries, articles, packages, bags, etc. shall be inspected and documentation verified prior to entry. All non-essential vehicle traffic will be avoided and rescheduled if possible.
- 5.5 No boarding ladders or gangways shall be left lowered on the offshore side of vessels and side ports shall be closed and secured when not in use.

**6. IDENTIFICATION PROCEDURES**

- 6.1 Terminal Management shall notify any vessels moored of the change to **Maritime Security Level 2**.
- 6.2 Terminal Management shall also immediately notify the PFSO of any change in the security level as advised by NDOT or the Port Authority.

**7. VEHICLE CONTROL/SECURITY**

- 7.1 Random (at least 10%) searches of vehicles (private or commercial) entering the Terminal, including contents of such vehicles, shall be conducted. Vehicles exiting may be searched.

7.2 Vehicles and Handling equipment will be secured with ignition keys or chains and padlocks.

7.3 Main Gate Security officers shall remind operators and drivers to lock parked vehicles and equipment and to institute a positive system of checking before they enter and drive any vehicles, forklifts or equipment.

## 8. **DECLARATION OF SECURITY**

8.1 Declaration of Security Procedures with vessels intending to berth at the Terminal shall be instituted by Terminal Management and carried out by the Operations Office/Duty Manager.

## 9. **TRAINING OF SECURITY FORCE AND THREAT AWARENESS FOR EMPLOYEES**

9.1 Emergency contingency plans shall be reviewed and additional training conducted as appropriate.

## **MARITIME SECURITY LEVEL 3 - THREAT OF IMMINENT ATTACK**

**Additional Measures for Maritime Security Level 3 condition: threat of unlawful act is probable or imminent and intelligence indicates that terrorists have chosen specific targets.**

### **1. THE TERMINAL WILL BE CLOSED DURING MARITIME SECURITY LEVEL 3 CONDITION**

- 1.1 Operations shall cease during Maritime Security Level 3. Port Authority and NDOT shall be advised when securing of operations has been completed.

### **2. PHYSICAL SECURITY**

- 2.1 All gates shall be closed.
- 2.2 Additional (plain clothes and/or uniformed) security officers shall be employed. Security officers will make continuous rounds and checks of restricted areas, waterfront areas, the main pier, vehicles, Terminal buildings and sheds and other areas of risk or vulnerability, paying close attention for suspicious packages, objects or tampering.
- 2.3 Security officers will report to on-site management staff on the security situation at the Port Facility on an hourly basis.
- 2.4 Any vessels alongside shall be capable of getting underway within two hours and shall have a "fire wire" (wire rope) lowered from the bow on the seaward side but no lower than 1 – 2 meters above the water or recessed cleat in hull for tug line.
- 2.5 Explosive screening of all ship stores shall be arranged with the Port Authority.
- 2.6 Where possible such objects as crates, trash containers, etc are to be removed from the Terminal Area.

### 3. ACCESS CONTROLS

- 3.1 Mail shall not be received at the Terminal without having been screened off site. All other articles, packages, bags, deliveries, etc. entering the Terminal shall be inspected.
- 3.2 All passenger/crew baggage to be screened.
- 3.3 Terminal entry/exit shall be limited to the main gate only.
- 3.4 All visitors, contractors, vendors and other Terminal guests shall be escorted to/from their destination. The escort may be a security officer or a company employee.
- 3.5 No boarding ladders or gangways shall be left lowered on the offshore side of vessels and side ports shall be closed and secured when not in use.

### 4. IDENTIFICATION PROCEDURES

- 4.1 Terminal Management shall notify any vessels moored of the change to **Maritime Security Level 3**.

### 5. INTERNAL SECURITY

- 5.1 Any non-essential work being conducted by contractors shall be cancelled or delayed. Terminal personnel shall closely supervise and escort any vendors or contractors performing essential repair work.

### 6. VEHICLE CONTROL/SECURITY

- 6.1 All delivery vehicles shall be opened and searched prior to entering the Terminal.
- 6.2 Cruise ships (not applicable – provide measures if applicable, e.g. searching/screening procedures).
- 6.3 Rail cars (not applicable - provide measures if applicable, e.g. searching/screening procedures).

**<CONFIDENTIAL WHEN COMPLETED>**

- 6.4 No barges or support boats shall be allowed to moor alongside and vessels without the Harbourmaster's permission and the Operations Manager's approval.
- 6.5 Only persons with Terminal or ship's official business (including crew) shall be authorized to embark or disembark a vessel.
- 6.6 Positive control for vessels shall be maintained with a security officer posted at the vessel gangway.

**7. COMMUNICATIONS AND ALARM SYSTEMS**

- 7.1 All communications and alarm systems shall be tested daily.

**8. TRAINING OF SECURITY FORCE AND THREAT AWARENESS FOR EMPLOYEES**

- 8.1 Emergency contingency plans shall be reviewed as appropriate. At the conclusion of the **Maritime Security Level 3** alert, a management review will be conducted to assure performance of all personnel and assess future procedural improvements.

## **ANNEX A – BOMB THREAT**

**A copy of this Annex shall be posted at all public phones on Terminal property and in all offices, boardrooms or equipment rooms and the like, adjacent to the telephones in those rooms.**

### **1. Receipt of Bomb Threat**

Bomb threats can be received in a variety of ways, including e-mail, phone call or message or verbal threat. Speak calmly to the person making the threat and obtain as much information as possible. Notify PFSO who will notify Duty Manager/Terminal Management and provide direction on next actions to be taken. All Terminal employees receiving a bomb threat must attempt to obtain the following information:

#### **1.1 Essential information:**

- What is it? (identify container and explosive);
- Where is it? (in the Terminal buildings, on board a ship, on jetty/pier, under a ship's hull, in a container, adjacent to a tank, etc);
- When is it set to go off?; and
- Is it booby trapped?;

#### **1.2 Additional information:**

- size and description of the bomb;
- amount and type of explosive;
- what organization planted it;

### **2. In addition, the person receiving the bomb threat call should note the following:**

- voice description (male/female, accent, tone (angry, anxious, hurried, calm) etc);
- call time and duration;
- background sounds (industrial noise, household, children, bar, restaurant, night club, etc); and
- any other information which could identify the caller or point of origin of the call.

3. **Reaction**

3.1 The initial reaction to receipt of a bomb threat will be dependent on circumstances and information obtained from the caller. Regardless of these factors, the incident will be treated initially as a threat and not as an emergency. Emergency action will be taken when the bomb is found or detonates. The person receiving the bomb threat is to contact the PFSO or the Duty Manager immediately and relay to them all the information listed above, and then follow their instructions on who next to call and what actions shall be taken.

4. Should, it be determined that in all probability, the bomb threat is not a hoax, the PFSO will direct the Main Gate/Security Office to:

- Inform the Port Authority/Harbourmaster, the local police, the Fire Department and other Emergency responders (bomb disposal, fire tug, etc) as required;
- Evacuate the threatened area;
- Prepare to direct Emergency Responders to search the area;
- Maintain control of the situation until relieved by the PFSO;
- Notify NIA, NDOT or SANDF as necessary.

G Mulder  
2004 March