

U.S. COAST GUARD



VESSEL SECURITY PLANNING GUIDE

INTRODUCTION

Shortly after the terrorist attacks of September 11th, the Secretary of Transportation directed the Coast Guard to take appropriate actions to reduce the vulnerability of the nation's marine transportation system. Since that time, the Coast Guard has implemented a number of safety and security zones as well as amending the requirements of vessels to provide advance notice of their arrival to ports in the United States.

In addition to the implementation of vessel movement control measures, the Coast Guard has been looking at ways to reduce the vulnerability of the transportation infrastructure used by the maritime industry. It is in this arena that Marine Safety Office Mobile has worked with various members of the maritime industry to create guidelines for the development of vessel and facility security plans. The results of that partnership have led to the creation of this guide, which provides for the development of a vessel security plan that can be tailored to the unique characteristics and location of the vessel while providing security measures through the full spectrum of threat to that vessel. While various measures of security may already be implemented onboard vessels and included in their International Safe Management (ISM) plans, this guide will supplement these existing measures to increase vessel security to a more productive level during high threat situations. While we have sought to incorporate the knowledge of various people, we are always seeking ways to make guides such as these better and so ask for your critical review and comment of this manual. Any comments or suggestions regarding this planning guide should be addressed to sotp@msomobile.uscg.mil.

I highly encourage you to take advantage of this document and prepare your vessel for the threat of terrorist or other illegal activities that seek to exploit your vessel's vulnerabilities. Our ability to assure the viability of the nation's marine transportation system can only be realized if we work together, building upon the partnerships we have formed. With your partnership, the ports along the Gulf Coast can lead the way for a safe and secure marine transportation system.

D.M. SMITH
Captain, U.S. Coast Guard
Captain of the Port

TABLE OF CONTENTS

I. VESSEL SECURITY	1
II. VESSEL SECURITY PLAN OUTLINE.....	3
III. MARITIME SECURITY LEVELS AND SECURITY MEASURES	13
IV. APPENDIXES	17
A. COAST GUARD ROLES AND RESPONSIBILITIES.....	17
B. VESSEL SECURITY MEASURES-BEST PRACTICES	20
V. REFERENCES	31

VESSEL SECURITY

Maritime Security can be defined as those measures employed to protect against seizure, sabotage, piracy, pilferage, annoyance, or terrorism. It can also be considered as embracing all measures taken to prevent interference within lawful operations. It must also include measures to prepare to respond to breaches of security. To this end, security personnel must adequately plan for participation in multi-agency maritime response operations with such agencies as local law enforcement, fire departments, private facilities, federal agencies, etc.

COAST GUARD SECURITY MEASURES

The Coast Guard Captain of the Port (COTP), in conjunction with other agencies, conducts maritime safety and security activities to safeguard vessels from accidents, negligence, illegal acts, terrorism and sabotage.

The Captain of the Port is responsible for ensuring the safety and security of assets within a geographic region, and has the authority to use available resources and manpower to protect all assets from maritime incidents. Additionally, the Coast Guard has identified three maritime security (MARSEC) levels that may be established within a COTP Zone. These levels aid in determining the resources and manpower that will be needed to be proactive in various situations. The MARSEC level is determined by the COTP, and are as follows:

MARSEC 1	Normal Operations. Vessels should be aware and vigilant of suspicious activities and possible threats. Vessels should employ the necessary measures to reduce the vulnerability and risk of their vessels from a marine incident. This represents the baseline level of security.
MARSEC 2	This security level is a moderately enhanced security posture. At this level, vessels will employ those additional measures identified in their security plan to reduce the vulnerability of and risk to their vessel from an incident. Vessels can expect the need for additional personnel and material resources when in port to reach this level.
MARSEC 3	This security level is a fully enhanced security posture resulting from specific threat to the maritime domain or marine transportation system. At this level, vessels will employ the full measures identified in their security plan.

Within each MARSEC level, the COTP has the authority to establish security and safety zones, reduce personnel access to vessels, and control operations on a vessel. These actions should support measures identified in the Maritime Security Levels and Security Measures section of this guide. The following are tactics that the COTP employs to ensure the overall waterside safety and security of a region.

- a. **Safety Zones**-Safety Zones protect structures, vessels, and water and shore areas by controlling access and activities within the zone. Most safety zones limit access during response to an emergency and can be set for an indefinite time period. Any person may request a security, safety, or regulated navigation area be established. Each request must be submitted in writing to either the COTP or appropriate District Commander

having jurisdiction over the location to be requested. The data required in the written request is specified in 33 CFR 165.5.

- b. **Security Zones**-Security Zones are designated areas of land, water, or land and water, which are established to prevent damage to any vessel or waterfront facility. These zones safeguard ports, harbors, territories, or waters of the United States from accidents or subversive acts by controlling access or movement of persons, vessels, and objects. These are used for national security interests rather than strictly safety considerations.
- c. **Harbor Patrols**-Harbor Patrols are used to detect suspicious activity and to determine if the level of security measures taken by vessel and facility owners and operators are adequate and sufficient to meet the existing threat level.

CONCLUSION

Security of vessels and the marine transportation system infrastructure can only be realized through the cooperative efforts of all parties involved. Just as the COTP has a variety of tools, including security plans to help ensure the safety and security of the maritime environment, so too do the other parties.

This guide is intended to assist vessel owners and operators in developing one of those tools; vessel security plans. The following sections include a vessel security plan outline and maritime security levels and security measures. These additional sections are intended to serve as a guide for vessel owners and operators in the development of their vessel security plan, thereby serving to minimize the vulnerability of the vessel to a maritime incident.

VESSEL SECURITY PLAN OUTLINE

This section provides an outline of a complete vessel security plan. In developing this plan, a vessel should be sure to fully address the physical security issues identified and the measures to be taken at each MARSEC Level. If a particular section does not apply to a vessel, it should be so stated in the plan and the appropriate reason why that section does not apply.

CONSIDERATIONS FOR ASSESSING VULNERABILITY

In formulating your ship's security plan take the following into consideration: the general layout of the ship; the location of areas which should have restricted access, such as bridge, engine room, radio-room, etc.; the location and function of each actual or potential access point to the ship; the open deck arrangement including the height of the deck above the water; the emergency and stand-by equipment available to maintain essential services; numerical strength, reliability and security duties of the ship's crew; existing security and safety equipment for protection of passengers and crew; and existing security measures and procedures in effect, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control and other appropriate systems.

OBJECTIVES.

The vessel security plan should cover procedures for periods of low, medium, and high threats that:

- a. Deter unauthorized access to the vessel and its restricted areas;
- b. Deter the introduction of prohibited weapons, incendiaries, and explosives aboard the vessel;
- c. Encourage vigilance, as well as general awareness of security, aboard the vessel;
- d. Provide adequate training to members of the crew for security aboard the vessel;
- e. Coordinate responsibilities for security between the vessel operator and the operator of each terminal at which the vessel calls;
- f. Provide information to members of the crew and to law-enforcement personnel, in case of an incident affecting security;
- g. Provide for amendment of the plan to address any known deficiencies; and
- h. Restrict the distribution, disclosure, and availability of information contained in the plan to those persons with an operational need to know.

OUTLINE:

The following outline is a guide for drafting vessel security plans:

- a. Vessel Security Officer. Identify the Vessel Security Officer by name:

Vessel Security Officer: _____

Responsibilities:

Security Functions:

- b. Basic information. (Security surveys should be conducted annually, or more frequently as needed in order to update plan).

Vessel Name: _____ Date: _____

Masters name: _____

Date of last security survey: _____

Date of last crew security indoctrination: _____

Vessel Owner:

Business Address: _____

Telephone Number:

Vessel Operator: _____

Business Address: _____

Telephone Number:

Owner/Operator: _____

Security Officer: _____

Business Address: _____

Telephone Number:

Vessel Description:
LOA: _____ Beam _____ Depth _____

Gross tonnage _____ Net Tonnage _____

Year built _____ Place _____

Recent vessel activity (types of cargo, shipping routes, ports of call, frequency of employment, security incidents): _____

Current intelligence threat for shipping route and ports of call:

Threat intelligence source (FBI, USCG, local authorities):

General Ship Layout: (Include all pertinent diagrams and sketches here).

Construction material: Hull _____

Superstructure _____ Decks _____

Average draft (light): FWD _____ AFT _____

Average draft (loaded): FWD _____ AFT _____

Average freeboard (light):
FWD _____ MIDSHIPS _____ AFT _____

Average freeboard (loaded):
FWD _____ MIDSHIPS _____ AFT _____

Accesses (number, type, and location of all doors, hatches, and ports):

Description and evaluation of access control:

- a. Inspection, control, and monitoring of crew, visitors, passengers and carry-on articles.

- b. Inspection, control and monitoring of cargo, ship's stores and baggage.

- c. General comments regarding access control:

Location of Restricted Areas: (Include all pertinent diagrams and sketches here):

Open Deck Arrangement (including the height of the deck above the ship - include all pertinent diagrams and sketches here):

Emergency and Standby Equipment available to maintain essential services:

Number of Ships Crew: _____

- c. Standard Operating Procedures. Any standard operating procedures related to security should be included in the plan.

Reporting procedures: _____

Watchstanding instructions: _____

Basic relief schedules: _____

- d. Alarms. Alarms, when used, should activate an audible or visual alarm when an intrusion is detected.

Alarm test date: _____

Alarm test results: _____

Is the alarm in a place continuously staffed by personnel with security responsibilities? _____

Procedure for sounding alarm at approach/boarding of attackers:

- e. Lighting. While in port, at anchor, or underway are the ship's deck and overside illuminated in periods of darkness and restricted visibility? _____

Does the lighting interfere with navigation lights and safe navigation?

Type, location and wattage of all fixtures: _____

- f. Communications. Communications should specify the kind of communications to use for a breach of security, an unlawful act or other emergency.

Shoreside means of communication provided to security personnel to communicate with vessel security officer, navigational bridge or communications center (radio, telephone or intercom)?

Procedures for establishing a distress signal peculiar to security, indicating a security alert:

- g. Screening. When screening is conducted, it may be done manually, electronically, or by an equivalent means acceptable to the Vessel Security Officer. Screening systems should be capable of detecting prohibited weapons, incendiaries, and explosives. Generally, vessel screening procedures should, at a minimum, include:
- (1) No person refusing to submit to a security screening at a point of access should board the vessel.
 - (2) Each person denied entry for refusing to submit to a security screening for suspicious reasons should be identified and reported to appropriate authorities.
 - (3) Security equipment should be kept in good working condition and checked monthly. Record of security equipment checks (should be maintained for at least 30 days after the date of the check). _____

 - (4) Procedures to ensure any defective or missing security equipment is reported immediately to the vessel security officer. _____

- h. Baggage. When passengers are carried, each piece of baggage should be marked, labeled or tagged, or otherwise identified as belonging to a particular passenger. During medium and high threat periods, it should be compared against the official passenger list of the vessel prior to being loaded aboard the vessel. No unidentified baggage should be permitted aboard the vessel.
- i. Identification. Each vessel operator should establish a system of identification and control of personnel for the vessel. The plan should cover the following procedures for:

- (1) Procedures for identifying each category of persons authorized to be aboard the vessel and each person authorized access to a restricted area aboard the vessel;

- (2) Permanent identification card procedures:

Issued to each member of the crew _____

Other employee of the vessel _____

Contains the cardholder's name _____

Age _____ Height _____ Weight _____

Eye color _____

Expiration date _____

Unique ID number _____

- (3) Procedures for providing a temporary identification card to each contractor, vendor, and other visitor authorized access to a restricted area: _____

- (4) Procedures for comparing each passenger authorized to board the vessel against the official passenger list.

- j. Designated Restricted Areas. Designated restricted areas should be outlined in the security plan. Restricted areas should be appropriately secured with access limited to authorized personnel. Each restricted area should be secured and conspicuously marked stating that the area has restricted access. Passenger vessels should

designate the following areas as restricted areas (it must be ensured that the required number of emergency exits are left unrestricted in case of fire):

- (1) Navigational bridge conspicuously marked? _____
- (2) Communications center conspicuously marked? _____
- (3) Engine room conspicuously marked? _____
- (4) Ships office conspicuously marked? _____
- (5) Master's safe conspicuously marked? _____

k. Firearms (number, type, stowage, and amount of ammunition on board). _____

l. Written security SOP's on board:

Moored dockside: Yes ___ No ___ Date _____

Moored dockside cargo ops: Yes ___ No ___ Date _____

At anchor: Yes ___ No ___ Date _____

At anchor cargo ops: Yes ___ No ___ Date _____

Underway: Yes ___ No ___ Date _____

Rendering assist. at sea: Yes ___ No ___ Date _____

Docking/undocking: Yes ___ No ___ Date _____

Rcvg/dschg pilots: Yes ___ No ___ Date _____

Rcvg ships stores: Yes ___ No ___ Date _____

Bunkering: Yes ___ No ___ Date _____

Rcvg official visitors: Yes ___ No ___ Date _____

Changing crew: Yes ___ No ___ Date _____

m. The vessel security plan should contain a coordination check sheet that is to be completed by the vessel and terminal Security Officer. This

checklist should clearly identify who is responsible for which security actions, paying particular attention to vessel/terminal interfaces. It must also contain a communication plan identifying how the vessel and terminal security will communicate any distress signals to be used during the vessels' stay.

MARITIME SECURITY LEVELS AND SECURITY MEASURES

Note: Once a Vessel has attained a MARSEC level above MARSEC 1, the vessel captain should inform the cognizant COTP.

MARSEC 1

Normal Operations. Vessels should be aware and vigilant of suspicious activities and possible threats. Vessels should employ the necessary measures to reduce the vulnerability and risk of their waterfront facility from a marine incident. This is the baseline level of security. “Vessel Captains should implement the following measures at all times when MARSEC ONE is designated.”

- a. **MEASURE 1.** Brief crew on threat, ship security, and security precautions to be taken while ashore.
- b. **MEASURE 2.** Security officers and responsible personnel should review security plans and keep them available.
- c. **MEASURE 3.** Enhance communications with pier personnel on minimizing pier access through control procedures. Thus identifying all personnel.
- d. **MEASURE 4.** Post signs in local languages to explain visiting and loitering restrictions.
- e. **MEASURE 5.** Inspect all personnel, hand-carried items, and packages before they come aboard. Where possible, screening should occur prior to passengers or cargo boarding vessel.
- f. **MEASURE 6.** Security alarms and communication systems should be established for restricted areas and at access points to the ship to complement guards and patrols with a response plan.
- g. **MEASURE 7.** At sea, cargo spaces should be controlled.
- h. **MEASURE 8.** Where practical, unused rooms or spaces should be kept locked.
- i. **MEASURE 9.** Regulate shipboard lighting to best meet the threat environment. Lighting should include illumination of the waterline on both sides of the vessel.
- j. **MEASURE 10.** Rig hawsehole covers and rat guards on lines, cables, and hoses. Consider using an anchor collar.
- k. **MEASURE 11.** Raise accommodation ladders, stern gates, and jacob ladders when not in use. Clear ship of all unnecessary stages, camels, barges, oil donuts, and lines.
- l. **MEASURE 12.** Conduct security drills to include bomb threat and repel boarder exercises.

- m. **MEASURE 13.** Review all plans, orders, personnel and logistic requirements related to the individual actions in MARSEC TWO for possible implementation.

MARSEC 2

This security level is an enhanced security posture. Vessels will employ those additional measures identified in their security plan to reduce the vulnerability of and risk to their vessel from an incident. Vessel Captains should implement the following measures when MARSEC TWO is designated:

- a. **MEASURE 14.** Maintain appropriate MARSEC ONE measures.
- b. **MEASURE 15.** Recommend vessels review liberty policy in light of the threat and revise it as necessary to maintain safety and security of ship and crew. Suggest a liberty curfew.
- c. **MEASURE 16.** Brief crews to ensure they understand the additional security requirements, to stop rumors and to prevent undue alarm.
- d. **MEASURE 17.** Remind all personnel to: (a) be suspicious and inquisitive of strangers, particularly those carrying suitcases or other containers; (b) be alert for abandoned parcels or suitcases; (c) pay closer attention to deliveries of stores; (d) be alert for unattended vehicles in the vicinity; (e) be wary of any unusual activities; (f) notify the Vessel Security Officer of any suspicions.
- e. **MEASURE 18.** Check seals on containers and other cargo.
- f. **MEASURE 19.** Under the supervision of an armed sentry, establish brow watch on pier to check identification and inspect personnel and baggage before personnel board ship. If available, employ metal and explosives detection equipment.
- g. **MEASURE 20.** Test communications with local authorities and U.S. Coast Guard.
- h. **MEASURE 21.** Conduct searches of the ship's hull and boats at intermittent intervals and immediately before it puts to sea.
- i. **MEASURE 22.** Hoist boats aboard when not in use. Small boats should remain ready for launch.
- j. **MEASURE 23.** Control and limit public visits.
- k. **MEASURE 24.** After working hours, reduce entry points to ship's interior by securing selected entrances from inside.
- l. **MEASURE 25.** Ensure all spaces not in regular use are secured and inspected periodically.
- m. **MEASURE 26.** If two brows are rigged, remove one of them.

- n. **MEASURE 27.** Maintain capability to get underway on short notice. Consider possible relocation sites. Rig brow/accommodation ladder for immediate raising/removal.
- o. **MEASURE 28.** Prepare fire hoses. Brief designated personnel on procedures for repelling boarders, small boats, and ultra-light aircraft.
- p. **MEASURE 29.** Monitor local communications (ship to ship, TV, radio, police scanners, etc.).
- q. **MEASURE 30.** Shore authorities should be informed if persons seeking access to the vessels are refused or decline to be subject to security measures.
- r. **MEASURE 31.** Review all plans, orders, personnel details and logistic requirements related to the implementation of the individual actions in MARSEC THREE.

MARSEC 3

This security level is a fully enhanced security posture and will normally be imposed when a specific threat exists to the maritime domain or marine transportation system. At this level, vessels will employ the full measures identified in their security plan. Vessel Captains should implement the following measures when MARSEC THREE is designated:

- a. **MEASURE 32.** Maintain appropriate MARSEC ONE and TWO measures.
- b. **MEASURE 33.** Be prepared to get underway on one (1) hour's notice or less. If conditions warrant.
- c. **MEASURE 34.** Man Signal Bridge or pilot house and ensure flares are available to ward off approaching craft.
- d. **MEASURE 35.** Augment existing security watches and deploy sentries to protect vessel.
- e. **MEASURE 36.** Place sentries on a superstructure level from which they can best cover areas about the ship.
- f. **MEASURE 37.** Activate anti-swimmer watch. (Portions of watch may already be implemented by previous MARSEC measures).
- g. **MEASURE 38.** Strictly, enforce entry control procedures and searches.
- h. **MEASURE 39.** Secure passageways, watertight doors, and cargo holds, main deck and below.
- i. **MEASURE 40.** Secure from the inside all unguarded entry points to the interior of the ship (it must be ensured that the required number of emergency exits are left unrestricted in case of fire).
- j. **MEASURE 41.** Rotate screws and cycle rudders at frequent and irregular intervals.

k. **MEASURE 42.** Rig additional firehoses.

APPENDIX A: COAST GUARD ROLES AND RESPONSIBILITIES

OVERVIEW

The U.S. Coast Guard has been responsible for the security of the ports of the United States since the enactment of the Espionage Act of 1917. It has performed port security duties during both World War I and World War II, while it was operating as a service within the Department of the Navy. Until 1950, port security was viewed as a wartime issue. In that year it was made a permanent program and the duties were again assigned to the U.S. Coast Guard.

PORT SAFETY AND SECURITY (PSS) PROGRAM

The PSS program originally emphasized security, expanded to include the safeguarding of ports, harbors, vessels, and waterfront facilities from accidents, negligence, terrorism, and sabotage. The port safety mission of the program is concerned primarily with the prevention of accidental damage to vessels and port facilities. This is generally accomplished through activities such as inspections, hazardous materials loading supervision, and cargo transfer monitoring. The port security mission is concerned with the prevention of intentional destruction, loss, or damage to port assets. During peacetime, port security is a law enforcement function. During wartime, however, port security can quickly change from being solely a law enforcement function to a military mission. Whether during peacetime or wartime, the Coast Guard primarily acts from law enforcement authority first. Port safety and security are closely related, mutually supportive, and are often conducted concurrently in field operations. Principal port security activities include:

- a. Monitoring port operations including certain types of marine events;
- b. Conducting harbor patrols to detect suspicious activity and to determine if the level of security measures taken by vessel and facility owners and operators are adequate and sufficient to meet the existing threat level;
- c. Surveying waterfront facilities to provide baseline data of facility capability that would be useful in emergency response;
- d. Establishing and enforcing security zones to safeguard vessels and port areas;
- e. Employing measures to control the movement of vessels within a geographic region.

STATUTORY AUTHORITY

The most basic authority for the Port Security Program is located in Title 50 of the U.S. Code section 191 with punitive provisions located in 50 U.S.C. 192. Section 191 is actually an amalgamation of two separate statutes, the Espionage Act of 1917 (Title II, 40 Statute 217) and the Magnuson Act of 1950 (64 Statute 427). Various Executive Orders and other directives also apply. Brief descriptions are given as follows:

- a. **Espionage Act of 1917**. The Espionage Act of 1917 provided the initial authority for a Coast Guard Port Security Program during periods of national emergency. Following

World War I, the program was discontinued until the outbreak of World War II. The program was again terminated in 1947.

- b. **Magnuson Act of 1950.** With the commencement of hostilities in Korea and the continuing Cold War, it was determined that broader authority was required for control of vessels and waterfront facilities. The Magnuson Act of 1950 (50 U.S.C. 191) amended the Espionage Act of 1917. It authorized the President to institute such measures and issues such rules and regulations necessary to "...govern the anchorage and movement of any foreign-flag vessels in the territorial waters; inspect such vessels at any time; safeguard against destruction, loss, injury from sabotage or other subversive acts, accidents, or other causes of a similar nature, vessels, harbors, ports, and waterfront facilities...subject to the jurisdiction of the United States..." whenever the President found the security of the U.S. endangered by "...war; invasion; potential subversive acts and/or disturbance of international relations."
- c. **Executive Order (E.O.) 10173.** President Truman, finding that the security of the U.S. was endangered, issued E.O. 10173 on 20 October 1950. This order directed implementation of the provisions of the Magnuson Act and prescribed certain port security regulations (33 CFR 6) to be enforced by the Coast Guard. This Order provided authority to prevent both intentional and accidental loss or destruction of vessels and waterfront facilities. It further directed all agencies and authorities of the United States Government and all state and local authorities to support, conform to, and assist in the enforcement of these regulations. This order was later amended by Executive Orders 10277, 10352, and 11249 and is pertinent today.
- d. **Ports and Waterways Safety Act of 1972 (PWSA).** From 1950 to 1972 the Magnuson Act and E.O. 10173 provided the basis for the Port Security Program. In enacting the PWSA, which was not contingent on our national security being endangered, Congress provided a broad permanent statutory basis for the exercise of non-defense aspects of port safety. The PWSA extends protection to life, property, and the marine environment as well as vessels and facilities. However, port security activities are interrelated with port security procedures for protecting vessels, harbors, ports, and waterfront facilities from intentional destruction, loss or injury due to subversive acts.
- e. **Executive Order (E.O.) 12656.** President Reagan signed E.O. 12656, "Assignment of Emergency Preparedness Responsibilities," on 18 November 1988. It set forth the national security emergency preparedness policy, to wit:

"The policy of the United States is to have sufficient capabilities at all levels of government to meet essential defense and civilian needs during any national security emergency. A national security emergency is any occurrence, including natural disaster, military attack, technological emergency, or other emergency, that seriously degrades or seriously threatens the national security of the United States. The President shall establish policy for the national security emergency preparedness. Pursuant to the President's direction, the National Security Council shall be responsible for developing and administering such policy. All national security emergency preparedness activities shall be consistent with the Constitution and laws of the United States and with preservation of the constitutional government of the United States.

Effective national security emergency preparedness planning requires: identification of

functions that would have to be performed during such an emergency; development of plans for performing these functions; and development of the capability to execute those plans.”

- f. **FEMA.** E.O. 12656 recognizes the Federal Emergency Management Agency (FEMA) as having a key role in national emergency preparedness in an advisory capacity to the National Security Council and in a coordination government. It contains general and specific planning requirements the Federal departments and agencies.
- g. **Title IX Public Law (P.L.) 99-399. The International Maritime and Port Security Act as Codified in 33 U.S.C. 1226.** This act amended the Ports and Waterways Safety Act, adding a new section-Section 7: Port, Harbor and Coastal Facility Security. This section authorizes the Secretary of Transportation to carry out measures to prevent or respond to an act of terrorism against an individual, vessel, or public or commercial structure that is subject to the jurisdiction of the U.S. and located within or adjacent to the marine environment, or a vessel of the U.S. or an individual on board that vessel.
- h. **Code of Federal Regulations.** regarding facility safety and security can be found within 33 CFR Subchapter K-*Security of Vessels*, Subchapter L-*Waterfront Facilities*, Subchapter N-*Outer Continental Shelf Activities*.

APPENDIX B: VESSEL SECURITY MEASURES-BEST PRACTICES

It is the primary responsibility of the master, security officer and crew of a vessel for the protection of and security of that vessel. However, the COTP *may prevent any person, article, or thing from boarding or being taken or placed in or upon a vessel whenever it appears that such action is necessary in order to secure such vessel from damage.* The goal of these measures is to detect intruders, delay their progress, and destroy their ability to continue. These are named as the three D's (Hawkes 1989). Vessels are required and expected to have adequate security. Security measures vary by vessel and facility but must be comprehensive enough to ensure the security through the full spectrum of threat. Examples of various best practices that can be taken by a vessel are as follows:

COMPANY SECURITY OFFICER

The Company should designate a Company Security Officer whose duties and responsibilities should include, but are not limited to:

- a. Determining the level of threats likely to be encountered by the vessel;
- b. Conducting a comprehensive security survey and regular inspections of the company's vessel(s);
- c. Developing and maintaining the Vessel Security Plan;
- d. Modifying the vessel security plan to address shortcomings and / or changes in security threats to a vessel;
- e. Encouraging security awareness and vigilance;
- f. Ensuring adequate training for personnel responsible for security of the vessel; and
- g. Coordinating implementation of the Vessel Security Plan with the appropriate Port / Facility Security Officers.

VESSEL SECURITY OFFICER

It is recommended that vessel operators appoint an officer, who could be the master, to be responsible for the security of each individual vessel; the ship security officer. Responsibilities of persons assigned as security officers at terminals and aboard vessels should include the following, but not be limited to:

- a. Conducting an initial comprehensive security survey in order to prepare a security plan, and thereafter regular subsequent security inspections of the facility/ship to ensure continuation of appropriate security measures;
- b. Implementing the facility/ship security plan;

- c. Recommending modifications to the facility/ship security plan to correct deficiencies and satisfy the security requirements of the individual facility/ship;
- d. Encourage security awareness and vigilance;
- e. Ensuring adequate training for personnel responsible for security;
- f. Reporting of occurrences of unlawful acts that affect the operation of the facility/ship.
- g. Coordinating the implementation of the facility/ship security plan with the competent operator security officers; and
- h. Coordinating with other national and international security services, as appropriate.

VESSEL CREW

The Master, Security Officer and crew should ensure the following items are superposed and implemented in order to cover procedures for periods of low, medium, and high threats:

- a. Deter unauthorized access to the vessel and its restricted areas;
- b. Deter the introduction of prohibited weapons, incendiaries, and explosives;
- c. Encourage vigilance, as well as general awareness of security;
- d. Provide adequate security training to employees/crew/passengers;
- e. Coordinate responsibilities for security between the vessel crew and the operators at each terminal at which the vessel embarks or disembarks passengers;
- f. Provide information to the Master, Security Officer, crew and to law-enforcement personnel, in case of an incident affecting security;
- g. Ensure any known deficiencies are reported and addressed in the plan;
- h. Restrict the distribution, disclosure, and availability of information contained in the plan to those persons with an operational need to know.

TRAINING AND DRILLS

Drills and exercises to ensure the adequacy of the vessel security plans should be conducted at periodic intervals. Vessel crew having specific security duties should know their responsibilities for vessel security as described in the Vessel Security Plan and should have sufficient knowledge and ability to perform their assigned duties. In addition, the Company Security Officer and Vessel Security Officer should have security training.

- a. Company Security Officer Training.** The Company Security Officer should have knowledge in the following, as appropriate:
- Security administration;
 - Relevant international conventions, codes and recommendations;
 - Responsibilities and functions of other involved organizations;
 - Relevant government legislation and regulations;
 - Risk, threat and vulnerability assessments;
 - Security surveys and inspections;
 - Vessel and port facility security measures;
 - Security training and education;
 - Recognition of characteristics and behavioral patterns of persons who are likely to commit unlawful acts;
 - Inspection, control and monitoring techniques;
 - Techniques used to circumvent security measures;
 - Recognition and detection of weapons, dangerous substances and devices;
 - Vessel and local port operations and conditions;
 - Security devices and systems; and
 - Methods of physical searches.
- b. Vessel Security Officer Training.** The Vessel Security Officer should have knowledge of the following, as appropriate:
- Vessel security plan and related emergency procedures;
 - Layout of the vessel;
 - Assessment of the risk, threat and vulnerability;
 - Methods of conducting security inspections;
 - Techniques used to circumvent security measures;
 - Operation of security equipment;

- Recognition of characteristics and behavioral patterns of persons who may be likely to commit unlawful acts;
- Recognition and detection of weapons, dangerous substances and devices;
- Port and vessel operations; and
- Methods of physical searches.

VESSEL SECURITY MEASURES AT SEA

Ship security plans should ensure that masters and crews are made fully aware of the risk involved during attacks by terrorists, pirates or armed robbers. In particular, they should address the dangers that may arise if a crew adopts an aggressive response to an attack. Early detection of a possible attack is the most effective deterrent. Aggressive responses, once an attack is underway and, in particular, once the attackers have boarded the ship, could significantly increase the risk to the ship and to those aboard.

- a. **Lock all restricted and vulnerable areas while at sea.** In accordance with the ship security plan, all doors allowing access to the bridge, engine room, steering gear compartments, officers' cabins and crew accommodation should be secured and controlled in affected areas and should be regularly inspected. The intention should be to establish secure areas which attackers will find difficult to penetrate.
- b. **Routing and Delaying Anchoring.** If at all possible, ships should be routed away from high-risk areas and, in particular, seek to avoid bottlenecks. If ships are approaching ports where there is a security risk on ships at anchor, rather than ships underway, and it is known that the ship will have to anchor off port for some time, consideration should be given to delaying anchoring by slow steaming or longer routing to remain well off shore thereby reducing the period during which the ship will be at risk. Contact with port authorities should ensure that berthing priorities are not affected. Charter party agreements should recognize that ships may need to delay arrival at risk areas when no berth is available for the ship or offshore loading or unloading will be delayed for a protracted period.
- c. **Practicing the Implementation of the Ship Security Plan.** The ship's crew should have practiced and perfected the procedures set down in the ship security plan. Alarm signals and procedures should have been thoroughly practiced. If instructions are to be given over the ship's address systems or personal radios, they must be clearly understood by those who may have not fully mastered the language in which the instructions will be given.
- d. **Watch Keeping and Vigilance.** Maintaining vigilance is essential. All too often the first indication of an attack have been when the attackers appear on the bridge or in the master's cabin. Advance warning of a possible attack will give the opportunity to sound alarms, alert other ships and the coastal authorities, illuminate the suspect craft, undertake evasive maneuvering or initiate other response procedures. Signs that the ship is aware it is being approached can deter attackers. When ships are in, or approaching areas where attacks take place, bridge watches and lookouts should be augmented. Additional watches on the stern or

covering radar “blind spots” should be considered. Companies should consider investing in low-light binoculars for bridge staff and lookouts. Radar should be constantly manned but it may be difficult to detect low profile fast moving craft on ship’s radars. A yacht radar mounted on the stern may provide additional radar cover capable of detecting small craft approaching from astern when the ship is underway. Use of an appropriately positioned yacht radar when the ship is at anchor may also provide warning of the close approach of small craft.

- e. **Communications.** The master should ensure that an authorized person responsible for communications is on duty at all times when the ship is in, or approaching, high-risk areas. Prior to entering areas where attacks have occurred and where the GMDSS installation on board does not have facility for automatically updating the “ship position” data from an associated electronic navigation aid, it is strongly recommended to enter the ship's position at regular intervals into the appropriate communications equipment manually. It is recommended that owners initiate the GMDSS INMARSAT "C" alarm program before entering affected areas for use when appropriate (MSC/Circ.805).
- f. **Radio Watch Keeping and Responses.** A constant radio watch should be maintained with the appropriate shore or naval authorities when in risk areas. Continuous watch should also be maintained on all distress and safety frequencies, particularly VHF Channel 16 and 2,182 kHz, as well as in any other channels or frequencies which could have been determined by local authorities for certain areas. Ships should also ensure all maritime safety information broadcasts for the area monitored. As it is anticipated that INMARSAT’s enhanced group calling system (EGC) will normally be used for such broadcasts using the Safety NET service, owners should ensure a suitably configured EGC receiver is continuously available when in, or approaching areas where there is risk of attack. Owners should also consider fitting a dedicated receiver for this purpose, i.e. one that is not incorporated into a Ship Earth Station used for commercial purposes to ensure no urgent broadcasts are missed.
- g. **Lighting.** Ships should use the maximum lighting available consistent with safe navigation, having regard in particular to the provisions of Rule 20(b) of the 1972 Collision Regulations. Bow and overside lights should be left on if it can be done without endangering navigation. Ships must not keep on deck lights when underway, as it may lead other ships to assume the ship is at anchor. Wide beam floods could illuminate the area astern of the ship. Signal projector lights can be used systematically to probe for suspect craft using the radar guidance if possible. So far as is practicable crew members on duty outside the ship's secure areas when in port or at anchor should avail themselves of shadow and avoid being silhouetted by deck lights as this may make them targets for seizure by approaching attackers. It has been suggested that ships should travel blacked out except for mandatory navigation lights. This may prevent attackers establishing points of reference when approaching a ship. In addition, turning on the ship's lights as attackers approach could alert them that they have been seen, dazzle them and encourage them to desist. It is difficult, however, to maintain full blackout on a merchant ship. The effectiveness of this approach will ultimately depend in part on the level of moonlight, but primarily on the vigilance of the ship's crew. While suddenly turning on the ship's light may alarm or dazzle attackers, it could also place the crew at a disadvantage at a crucial point through temporary loss of their night vision. On balance, this approach cannot be recommended.

- h. Alarms.** Alarm signals, including the ship's whistle, should be sounded on the approach of attackers. Alarms and signs of response can discourage attackers. Alarm signals or announcements which provide an indication at the point at which the attacker may board, or have boarded, may help crew members in exposed locations select the most appropriate route to return to a secure area.
- i. Evasive Maneuvering and Use of Hoses.** Provided that navigational safety allows, masters should consider "riding off" attackers craft by heavy wheel movements as they approach. The effect of the bow wave and wash may deter would-be attackers and make it difficult for them to attach poles or grappling irons to the ship. Maneuvers of this kind should not be used in confined or congested waters or close inshore or by ships constrained by their draught in the confined deep-water routes found, for example, in the Malacca and Singapore Straits. The use of water hoses should also be considered though they may be difficult to train if evasive maneuvering is also taking place. Water pressures of 80 lb per square inch and above have deterred and repulsed attackers. Not only does the attacker have to fight against the jet of water but the flow may swamp his/her boat and damage engines and electrical systems. Special fittings for training hoses could be considered which would also provide protection for the hose operator. A number of spare fire hoses could be rigged and tied down to be pressurized at short notice if a potential attack is detected. Employing evasive maneuvers and hoses must rest on a determination to successfully deter attackers or to delay their boarding to allow all crew members to gain the sanctuary of secure areas. Continued heavy wheel movements with attackers on board may lessen their confidence that they will be able to return safely to their craft and may persuade them to disembark quickly. However, responses of this kind could lead to reprisals by the attackers if they seize crew members and should not be engaged in unless the master is convinced he can use them to advantage and without risk to those on board. They should not be used if the attackers have already seized crew members.

VESSEL SECURITY MEASURES WHEN LIGHTERING OFFSHORE

The following, additional security precautions have been adopted by the Industry Task Force on Offshore Lightering (ITOL), and should be followed by all vessels engaged in lightering operations in the Gulf of Mexico:

- a. For all tank ships (ships-to-be-lightered and lightering service ships):**
- Review your vessel's Piracy Contingency Plan and adopt appropriate precautions, as deemed appropriate.
 - Keep additional lighting on decks and have bridge watches make frequent checks of the sides of the vessel and the stern from the bridge wings for suspicious activities. Also, have bridge watches remain especially alert for suspicious vessel activity in their vicinity by making frequent radar and visual observations.
 - Establish hourly perimeter patrols of the vessel to make checks of the cargo deck, bow and stern areas for suspicious activities and report findings to the bridge watch.
 - Make regular status checks with the bridge watch of the tankship with which transfer operations are being conducted.

- b. **For all lightering support vessels: (fender/hose vessels):** Maintain a continuous bridge watch to surveil the vicinity of the ships engaged in lightering operations, by visual means and radar, and report all observations to the service ship. Make periodic patrols of the lightering area and inspect the entire waterline of both vessels at least once every 4 hours.

VESSEL SECURITY IN PORT

The vessel security officer should take advantage of such information as is available to assess the threat of ports on which the ship will call and about the port facilities and their security measures. Prior to entering port, vessel security officers should ensure that pre-arrival checks are incorporated into their ship security plans. In addition, it is recommended that upon the vessel's arrival to port, the vessel security officer and terminal security officer meet and address areas where ship and terminal interface.

- a. **Pre-Arrival Considerations.** The following should be checked prior to entering port.
- Check identities of all personnel embarking and disembarking the vessel.
 - Check all passenger cabin baggage and consider random check of crew baggage.
 - Check all passenger hand baggage.
 - Check all stores and provisions.
 - Lock all restricted areas while at sea and in port.
 - Secure all vulnerable areas while at sea and in port.
 - Search all areas of the ship prior to arrival.
 - The need for enhanced surveillance and the use of lighting, and detection equipment.
- b. **Additional Considerations.** The following items should also be considered in the event of an incident:
- Crew responses, if the potential attack is detected or an attack is underway.
 - The radio alarm procedures to be followed, and
 - The reports to be made after an attack or an attempted attack.
- c. **Declaration of Security Inspection.** It is recommended that the vessel security officer and terminal security officer meet upon the vessel's arrival to ensure a unity of efforts where the ship and terminal security efforts interface. At MARSEC level 2 and 3, the ship and terminal security officer should complete a declaration of security inspection. This document consists of baseline measures the terminal and vessel have taken to prevent security incidents from occurring. A sample document is provided on the next page.

DECLARATION OF SECURITY INSPECTION

Complete this form upon vessel's arrival at terminal.

Terminal	Location		
Vessel	Date/Time		
	Terminal	Vessel	
1. Vessel and Terminal Security Plans reviewed and understood by both parties.			
2. Security drills conducted. (Repel Boarders on Vessel, Bomb Threat on Vessel and Terminal)			
3. Adequate communications set between terminal and vessel for security issues.			
4. Communications made with local, national and/or international authorities concerning possible security issues.			
5. Access control in place at terminal and vessel entrances. Incoming stores, provisions and personnel checked and monitored.			
6. Cargo operations monitored. As applicable, ensure that weights and quantity of cargo matches with manifests/bills of lading and that container seals have not been tampered with.			
7. Barriers deployed if necessary to keep vehicles away from ship.			
8. Warning Signs displayed explaining visiting and loitering restrictions.			
9. Adequate security lighting in place on terminal and vessel.			
10. Restricted areas locked and periodically checked/Signs posted on restricted areas.			
11. Security alarms tested and working properly on terminal and vessel.			
12. Waterside security measures in place by vessel. (Jacob ladders, stern gates, and accommodation ladders raised; vessel cleared of all unnecessary items such as lines, camels, barges, and staging).			
13. Waterside security measures in place by terminal. (Boat exclusion zones enforced).			
14. Vessel pier side security in place. (Rat guards on lines, cables and hoses; anchor collars used if available).			
15. Security patrols or watches conducted on terminal and vessel.			
The Terminal and Vessel Security Officers should initial each item above, as applicable, and then sign below. A copy should be kept in the Terminal and Vessel Security records.			
I do certify that I have personally inspected this terminal or vessel with reference to the recommendations listed above.			
Terminal Security Officer:		Date/Time:	
Vessel Security Officer:		Date/Time:	

- d. **Barge Fleeting Areas.** Barge compartments should be secured when possible upon delivery to fleeting areas. It is recommended that access controls such as 24-hour guards with random security checks be posted for barge fleeting areas pier side. In addition, security patrols should be conducted at the waterside in order to detect any suspicious activity that may occur.
- e. **Anti-Swimmer Devices.** Vigilance is essential to deter swimmer attacks. Watches should be conducted randomly at frequent intervals to include shore and water sweeps of the berth, ship's waterline, underneath piers, around storm drains and other potential hiding places. Hawsehole covers and rat guards should be placed on lines, hoses and cables upon entry to port. Anchor collars should be utilized when available. Accommodation ladders, Jacob ladders, and stern gates should be raised when not in use. Clear the ship of all unnecessary stages, camels, barges, oil donuts, lines, and raise all small boats when not in use. Conduct security drills to include bomb threat and repel boarder exercises.

INCIDENT REPORTING

Each breach of security, unlawful act, or the threat of an unlawful act against a vessel, terminal, or the persons aboard them should be reported as soon as possible. For incidents that occur within the jurisdiction of the United States, the operator or the operator's representative should make the report to the cognizant COTP and to the local office of the Federal Bureau of Investigation.

For U.S. flag vessels or vessels regulated under 33 CFR Part 120, incidents that occur outside of the jurisdiction of the United States shall be reported as soon as practicable to Commandant (G-MOR), 2100 Second Street, SW., room 2100, Washington, DC 20593. Each report must include, to the extent known, the following information (see sample document on page 29):

- a. The vessel's name;
- b. The vessel's flag;
- c. The name of the vessel's master;
- d. If the vessel is moored to a passenger terminal, the name of the terminal security officer;
- e. An account of the incident;
- f. The date, time, and place of the incident;
- g. The number of alleged offenders;
- h. A description of how any weapon, incendiary, or explosive involved was concealed and used;
- i. The method used to introduce any prohibited weapon, incendiary, or explosive into or onto the vessel;
- j. A description of any weapon, incendiary, or explosive involved;

- k.** A description of how security was breached;
- l.** A statement of what measures have been taken or will be taken to prevent another such incident; and
- m.** Each report should stay on file with the security plan for a period of two years. All reports shall be used by the person preparing the ship security survey.

INCIDENT REPORTING WORKSHEET			
Date of Occurrence:		Suspected Terrorist Act <input type="checkbox"/> Yes <input type="checkbox"/> No	
		Time of Occurrence (Local):	
<input type="checkbox"/> Vessel Incident	<input type="checkbox"/> Terminal Incident	<input type="checkbox"/> Personnel Incident	<input type="checkbox"/> Other Incident
Vessel Data			
Name of Vessel:	Official No.	Nationality:	Vessel Type:
Location of Incident:		Name of Master or Person in Charge:	
Terminal Data			
Terminal Name:	Location of Terminal (Address):		City:
Terminal Type: <input type="checkbox"/> Passenger	<input type="checkbox"/> Cargo	<input type="checkbox"/> Rail	<input type="checkbox"/> Other
Name of Security Company:	Security Officer:		Phone:
Personnel Incident Data			
Type of Act: (Explain i.e. Death, Injury, Criminal Act, etc)			
Victim No. 1 Name:	Address:		Phone No.
Victim No. 2 Name:	Address:		Phone No.
Victim No. 3 Name:	Address:		Phone No.
Other Information			
Was a Weapon involved? <input type="checkbox"/> Yes <input type="checkbox"/> No		Drug involvement? <input type="checkbox"/> Yes <input type="checkbox"/> No	
		Alcohol involvement? <input type="checkbox"/> Yes <input type="checkbox"/> No	
Was an Explosive or Incendiary Device Used? <input type="checkbox"/> Yes <input type="checkbox"/> No		If Yes, where was it located?	
Description of Device:		How was it brought into Vessel or Terminal?	
How many alleged offenders were involved?		Can you provide a description of the alleged offenders? If so, enter descriptions in narrative summary on page 2	
Circumstances which allowed this incident to occur:		Preventative measures taken since this incident:	

Narrative Summary of Incident

Please provide a detailed description of the events which occurred during this incident:

Name of Individual submitting Report:	Address:	Phone:
The Above Statement is True and Correct	Signature:	Date:

REFERENCES

- Hawkes, K.G. Maritime Security. Cornel Maritime Press. Centreville, MD:
1989. Maritime Security Council, U.S. Department of Transportation, United States Maritime Administration, and the U.S. Coast Guard. International Perspective on Maritime Security. Washington, D.C.
- International Chamber Of Shipping, 21 November 2001, Guidance For Shipowners, Ship Operators And Masters On The Protection Of Ships From Terrorism And Sabotage.
- International Maritime Organization, MSC CIRC.443, 26 September 1986, Measures to prevent unlawful acts against passengers and crews on board ships.
- International Maritime Organization, MSC CIRC.623 Rev 2, 20 June 2001, Piracy and Armed Robbery Against Ships.
- Security for Passenger Vessels and Passenger Terminals COMDTPUB P16700.
- U.S. Code of Federal Regulations Title 33 Part 160: *Temporary Requirements for Notification of arrival in U.S. Ports*.
- U.S. Customs Service, Government Publications Office, 1989, Standards for Cargo Security.