



NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. **4 02**

Subj: SECURITY FOR PASSENGER VESSELS AND PASSENGER TERMINALS

Ref: (a) Title 33 CFR part 120 and 33 CFR part 128  
(b) Marine Safety Manual Vol. VII, Port Security, COMDTINST M16000.12 (Series)  
(c) International Maritime Organization MSC/Circ. 443, "Measures to Prevent Unlawful Acts Against Passengers and Crews On Board Ships"

1. PURPOSE. This Navigation and Vessel Inspection Circular (NVIC) establishes new guidelines for developing security plans and implementing security measures for passenger vessels and passenger terminals that must comply with 33 CFR part 120 and 33 CFR part 128. These guidelines accompany and interpret the requirements in current regulations and are for use in achieving the appropriate level of security for passenger vessels and passenger terminals per ref (a), (b), and (c).

2. ACTION.

a. Owners and operators of passenger vessels and/or passenger terminals who must comply with 33 CFR part 120 and 33 CFR part 128 should revise their security programs to reflect the security measures and performance standards identified in enclosure (1). Security plans should be amended within 30 days of the publication date for this NVIC. Commanding Officers of Marine Safety Offices, Captains of the Port (COTPs) and the Commanding Officer Marine Safety Center may extend the amendment date to allow for adequate time for proper notification, however the amendment date should not be extended more than 60 days past the publication date.

b. Commanding Officers of Marine Safety Offices, COTPs and the Commanding Officer Marine Safety Center should utilize the guidelines in this circular when examining security programs required by 33 CFR part 120 and 33 CFR part 128. COTPs are directed to validate vessel plan arrangements upon approval by the MSC. This circular will be distributed by electronic means only. It is available on the World Wide Web at <http://www.uscg.mil/hq/g-m/nvic/index.htm>.

DISTRIBUTION -SDL No. 139

	A	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	U	v	w	X	y	z
A																										
B		2	10		1			1						132	1			1								30
C												1														
D	1	1		1							1															
E															1											
F																										
G																										
H																										

NON STANDARD DISTRIBUTION: B/a G-MOC, G-MO-1, G-MSE, MSC(1)

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. **4 02**

- c. Enclosure (1) to this NVIC contains Sensitive Security Information (SSI), which is controlled under the provisions of 49 CFR Part 1520. A public version of enclosure (1) that does not contain SSI material will be available for viewing or download from the US Coast Guard's Internet site. The SSI material in enclosure (1) will be distributed separately via electronic means to the Area(m), District(m), COTPs, the Commanding Officer of the National Maritime Center, and the Commanding Officer of the Marine Safety Center. Members of the maritime industry, members of federal, state, or local law enforcement, and other parties that can demonstrate a need to know may submit a written request for the SSI material to the cognizant COTP, the Commanding Officer Marine Safety Center, or Commandant (G-MP). Written requests for this information must contain the following statement:

"I ACKNOWLEDGE THAT SSI MATERIAL SHALL NOT BE RELEASED WITHOUT THE WRITTEN PERMISSION OF THE UNDER SECRETARY OF TRANSPORTATION FOR SECURITY, WASHINGTON, DC 20590. FURTHER, I ACKNOWLEDGE THAT THE UNAUTHORIZED RELEASE OF SSI MATERIAL MAY RESULT IN CIVIL PENALTY OR OTHER LEGAL ACTION."

3. DIRECTIVES AFFECTED. COMDTPUB P16601, NVIC 3-96, CH-1 is cancelled. Marine Safety Manual Vol. VII, Port Security, COMDTINST M16000.12, Section 2-C.1.b, "Physical Security Assessments," and Section 2-D, "Physical Security Standards" remain in effect, but will be revised in the future to reflect the information contained in this NVIC.

4. BACKGROUND.

- a. The September 11, 2001 terrorist attacks on the United States demonstrated the ability of international terrorists to attack the U.S. Through existing regulatory and industry requirements, the cruise ship industry was better prepared than other segments of the maritime industry, but the response to the threat showed improvements are necessary. This NVIC builds upon the pre- September 11 standards and provides a more comprehensive security program to protect against future threats.
- b. This NVIC is a compilation of the existing regulations, NVIC 3-96, Change 1, and the International Maritime Organization's Maritime Safety Committee Circular 443, "Measures To Prevent Unlawful Acts Against Passengers and Crews On Board Ships" [reference (c)]. It is intended to serve as a single point of information for developing, implementing, and evaluating security programs required by 33 CFR part 120 and 33 CFR part 128.
- c. This NVIC renames and redefines the existing security levels, adds a fourth security level, identifies new definitions, and provides additional security measures with the expected performance standard for each measure. It elevates the baseline security standards to meet the threat of terrorism and sets consistent national security measures aboard passenger ships and passenger terminals.

5. DISCUSSION.

- a. Enclosure (1) establishes guidance on the new national security standard for passenger vessels and terminals regulated under 33 CFR part 120 and 33 CFR part 128. The policy outlined in these guidelines addresses security gaps in the implementation of the current regulations. It would be unlikely for a COTP to require additional security measures for a passenger vessel and/or terminal regulated by either 33 CFR part 120 or 33 CFR part 128, unless that COTP is aware of a specific threat against a particular vessel, terminal or port complex.
- b. The guidelines provide examples of criteria that will be considered by the Coast Guard during review and examination of security programs required by 33 CFR part 120 and 33 CFR part 128. In evaluating compliance with these new guidelines, the Coast Guard may recognize equivalent standards or alternatives. As an example, the benefit that may be gained by having installed baggage-screening equipment removed from the vessel at each port may be minimal when compared to the damage incurred to the equipment. Other operational measures, such as maintaining the equipment in a minimally manned room, may achieve the desired results less intrusively.
- c. The U.S. is working closely with our international partners through the International Maritime Organization (IMO) to improve vessel, port, facility, and offshore platform security guidelines. A number of additional security measures are currently being considered by IMO, and may result in additional security requirements in the future.

6. APPLICABILITY.

- a. Passenger Vessels: The guidance in the enclosures applies to all passenger vessels over 100 gross tons, carrying more than 12 passengers for hire; making voyages lasting more than 24 hours, any part of which is on the high seas; and for which passengers are embarked or disembarked in the United States or its territories. It does not apply to ferries that hold Coast Guard Certificates of Inspection endorsed for "Lakes, Bays, and Sounds", and that transit international waters for only short periods of time, on frequent schedules.
- b. Passenger Terminals: The guidance in the enclosures applies to all passenger terminals in the United States or its territories when being used for the assembling, processing, embarking, or disembarking of passengers or baggage for passenger vessels over 100 gross tons, carrying more than 12 passengers for hire; making a voyage lasting more than 24 hours, any part of which is on the high seas. It does not apply to terminals when serving ferries that hold Coast Guard Certificates of Inspection endorsed for "Lakes, Bays, and Sounds", and that transit international waters for only short periods of time, on frequent schedules.

7. PROCEDURES.

- a. Passenger vessel/terminal owners should amend their plans to reflect security measures and performance standards in Enclosure (1). In accordance with the current plan review procedures, amended vessel security plans shall be submitted to the Commanding Officer of the Marine Safety Center for review; amended terminal plans shall be submitted to the cognizant Captain of the Port for review.
- b. To expedite the review process, the Coast Guard will review the plans in two stages. The preliminary review will ensure basic updates are completed to the plans. Enclosure (2) identifies those items that need to be addressed for an operator to receive preliminary approval. If a plan does not meet the items addressed in Enclosure (2), the plan must be returned for immediate correction. Once preliminary approval is completed, the plan holder will be allowed to operate pending final approval of the plan.
- c. Final approval will be completed pursuant to normal review procedures. Discrepancies identified during the final review should be returned for revision while providing adequate time for correction. The Marine Safety Center review process (Procedure H2-27) can be found at: <http://www.uscg.mil/hq/msc/PRGuidance/h2-27.pdf>.



PAUL J. PLUTA  
ASSISTANT COMMANDANT FOR  
MARINE SAFETY, SECURITY &  
ENVIRONMENTAL PROTECTION

Encl: (1) Detailed Security Guidelines  
(2) Interim Review Checklist

## Security Guidelines for Passenger Vessels and Passenger Terminals

1	Definitions	1
2	Security Program	2
2.1	Provide Increasing Security Measures for Multiple Threat Levels	3
2.2	Designated Security Officer	3
2.2.1	Company Security Officer	3
2.2.2	Ship/Terminal Security Officer	3
2.3	Development of a Security Plan	4
2.4	Provide for the Safety and Security of Persons and Property	4
2.4.1	Security Briefs	4
2.4.2	Security Inspections	5
2.4.3	Secure Communications	5
2.4.4	Additional Security Measures	6
2.5	Prevent or Deter Carriage of a Prohibited Weapon, Incendiary, or Explosive	6
2.5.1	Prohibited Weapons	6
2.5.2	Screening Standards	7
2.5.3	Screening Procedures	7
2.6	Prevent or Deter Unauthorized Access to the Ship & Restricted Areas	9
2.6.1	Personnel Security	9
2.6.2	Terminal Physical Security	12
2.6.3	Ship Physical Security	17
2.6.4	Waterside Security	19
2.7	Coordination of Security Activities Between the Terminal and Ship	19
2.7.1	Communication	20
2.7.2	Liaison with Law Enforcement	20
2.7.3	Terminal Security at Calling Ports	20
2.8	Training for Security Personnel	21
2.8.1	General	21
2.8.2	Criteria	21
2.8.3	Terminal Security Personnel	21
2.8.4	Ship Security Personnel	23
2.8.5	Law Enforcement Personnel	24
2.8.6	Security Drills and Exercises	24
2.9	Pre-Hiring Evaluation of All Terminal Security Personnel (Terminal Only)	24
3	Reports of Security Violations	25
3.1	Ship Security Violation Reports	25
3.2	Terminal Security Violation Reports	27
3.3	Standard Report Form	27
4	Security Plan	27
4.1	Security Plan Details	27
4.1.1	Security Program Personnel and Procedures	27
4.1.2	Security Survey	28
4.2	Security Plan Review Requirements	32
4.2.1	Ship Security Plan Review	32
4.2.2	Terminal Security Plan	33
4.2.3	Security Plan Assessments	35

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

## **1 Definitions**

*Calling Port* refers to a port where the ship moors (or anchors) and passengers and crew are allowed to leave the ship to visit the port. Passenger baggage and ship stores will not normally be loaded or off-loaded at calling ports.

*Captain of the Port (COTP)* means the Coast Guard officer designated by the Commandant to command a Captain of the Port Zone as described in the 33 CFR regulations, or an authorized representative.

*Commandant* means the Commandant of the U.S. Coast Guard as described in 33 CFR 125.01, 46 CFR 1.01-05.

*Company Security Officer* means a company official from the ship operator who will be responsible for developing, maintaining, and enforcing the company security policies as set out in this document.

*Disembark* means, for the purposes of these guidelines, any time that the crew or passengers leave the ship, be it a port call or final destination.

*Embark* means, for the purposes of these guidelines, any time that the crew or passengers board the ship, be it a port call or initial boarding of the ship.

*FBI* means the Federal Bureau of Investigation.

*High seas* means all waters that are neither territorial seas nor internal waters of the United States or of any foreign country as defined in Part 2, Subpart 2.05, of Title 33, Code of Regulations.

*Marine Safety Center (MSC)* means the Commanding Officer of the Coast Guard Marine Safety Center.

*Maritime Security (MARSEC) Condition A* means the lowest level of security for the large passenger ship industry. This level of security allows a reduction in the security activities on the basis that the ship is in a period of extended maintenance (e.g., dry-docking) when there are no passengers onboard.

*Maritime Security (MARSEC) Level I* means the new maritime security normalcy. This is the risk level for which protective measures must be maintained for an indefinite period of time; in other words, these are the normal, every day security measures.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

*Maritime Security (MARSEC) Level II* means there is a heightened threat of an unlawful act against a port, facility or vessel and intelligence indicates that terrorists are likely to be active within a specific area or against a specific class of target. This risk level indicates that a particular segment of the industry may be in jeopardy but that no specific target has been identified. Additional protective measures may be expected to be sustained for substantial periods of time.

*Maritime Security (MARSEC) Level III* means the threat of an unlawful act against a port, facility or terminal is probable or imminent. Intelligence may indicate that terrorists have chosen specific targets, though it may not be possible to identify such targets. Additional protective measures are not intended to be sustained for substantial periods of time.

*Operator* means the person, company, or governmental agency, or the representative of a company or governmental agency, which maintains operational control over a passenger ship or passenger terminal.

*Passenger terminal* means any structure used for the assembling, processing, embarking, or disembarking of passengers or baggage for ships subject to this part. It includes piers, wharves, and similar structures to which a ship may be secured; land and water under or in immediate proximity to these structures; buildings on or contiguous to these structures; and equipment and materials on or in these structures.

*Unlawful act* means an act that is a felony under U.S. federal law, under the laws of the states where the ship is located, or under the laws of the country in which the ship is registered.

*Voyage* means the passenger ship's entire course of travel, from the first port at which the ship boards passengers until its return to that port or another port where the majority of the passengers are offloaded and terminate their voyage.

## **2 Security Program**

A comprehensive security program is essential to the safe transport of persons and property by ships. This section provides further explanation and guidance on achieving compliance with the intent of the regulations. The requirements for ships and terminals are similar. This section addresses both situations simultaneously and breaks down the individual components of the security program. In order to be effective, the ship and terminal security programs must be coordinated. Flexibility and coordination are particularly important for passenger facilities/terminals at calling ports (i.e. ports where the ship moors, or anchors, and passengers and crew are allowed to leave the ship to visit the port.). Section 2.7.3 of this document provides specific guidance for coordinating and documenting security at calling ports.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

## **2.1 Provide Increasing Security Measures for Multiple Threat Levels**

The security program must be scalable in order to provide increasing levels of security at increasing threat levels. The U.S. Coast Guard has identified four threat levels for the large passenger ship industry: A, I, II, III. The threat levels are defined in section 1 of this guide. The scalable activities that occur at each threat level are contained in the various activity specific sections of this guide.

## **2.2 Designated Security Officer**

### **2.2.1 Company Security Officer**

The company security officer should be responsible for, but not limited to:

- Conducting an initial comprehensive security survey of the ship/terminal;
- Overseeing the development of the ship security plan and the integration with the terminal security plan;
- Approve modifications to the ship security plan in order to correct deficiencies, ensure consistency with the terminal security plan, and satisfy the security requirements;
- Encouraging security awareness and vigilance; and
- Ensuring that adequate training has been provided for security personnel.

### **2.2.2 Ship/Terminal Security Officer**

Both the passenger ship and passenger terminal must have a security officer designated by name in their respective plan. Where the terminal security plan is contained solely in the annex to the ship security plan, the terminal security plan shall list an appropriate liaison for security activities at that terminal.

The ship/terminal security officer should be responsible for, but not limited to:

- Regular inspections of the ship/terminal;
- Implementing and maintaining the security plan;
- Proposing modifications to the security plan to correct deficiencies and satisfy the security requirements of the ship;
- Encouraging security awareness and vigilance onboard the ship/within the terminal;
- Ensuring that adequate training has been provided for security personnel;
- Reporting all occurrences or suspected occurrences of unlawful acts as required by the regulations and as discussed in section 3 of this guide.
- Coordinating implementation of the ship and terminal security functions and plans.



## **2.3 Development of a Security Plan**

An effective security program relies on detailed procedures that clearly indicate the preparation, prevention, and response activities that will occur at each threat level and the organizations, or personnel, who are responsible for carrying out those activities. These procedures should be documented in the form of an overall security plan. While the security plan need not include all of the detailed procedures for the various activities, these procedures should be clearly referenced within the framework of the plan. This latter step is necessary in order to establish a common link between the overall awareness, training, and execution of the security program.

Security plans should be developed for each ship. Ship security plans should be sufficiently flexible to take into account the level of security reflected in the terminal plan for each port at which the ship intends to call. In this regard, there needs to be an agreement between the ship and the terminal as to which entity will perform specific security functions. These agreements should be summarized in annexes to the ship security plan.

Terminal security plans should be developed and maintained for each passenger terminal regardless of the scope of the operation. These plans should contain an appropriate degree of security based upon local conditions and capabilities.

Section 4 of this document describes the detailed guidance for the development and review of ship and terminal security plans.

## **2.4 Provide for the Safety and Security of Persons and Property**

The security program must provide for the safety and security of persons and property. General safety and security can be accomplished through improved awareness of the threat level and the physical condition of the ship and terminal. Tables 2-1 and 2-2 outline the scheduling of security briefs and security inspections.

### **2.4.1 Security Briefs**

Security awareness training, as described by section 2.8 of this document should be conducted for ship/terminal employees at all Maritime Security Levels. The following table provides additional guidance as to when updated threat information should be provided to the crew and passengers.

**Table 2-1**

<b>MARSEC LEVEL</b>	<b>A</b>	<b>I</b>	<b>II</b>	<b>III</b>
<b>INFORMATION</b>				
Security brief to all crew/terminal employees about the threat				

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

Security brief to passengers about the specific threat



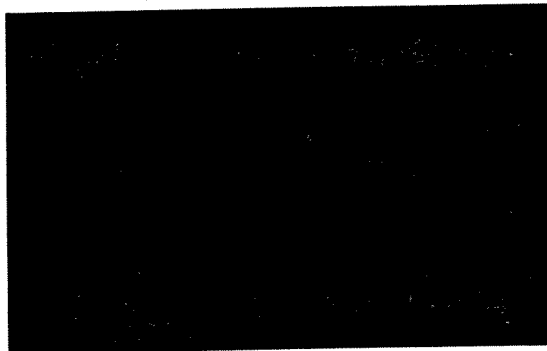
## 2.4.2 Security Inspections

Table 2-2

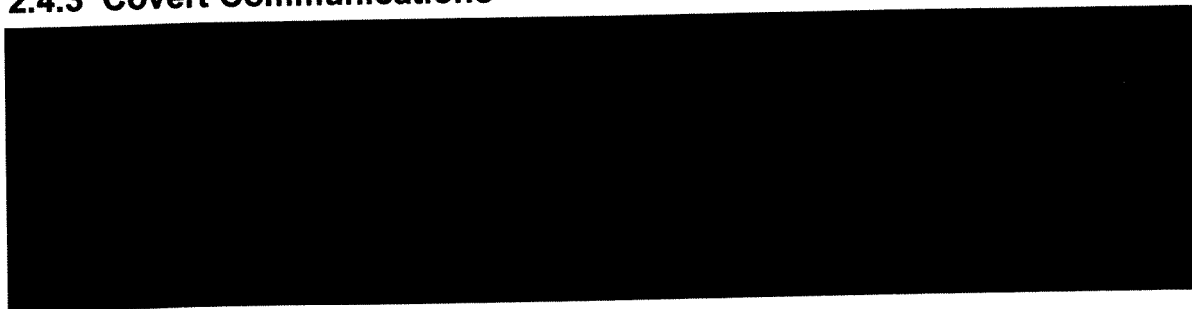
MARSEC LEVEL	A	I	II	III
<i>SEARCHING THE SHIP</i>				
Selected area search prior to sailing				
Full search as per ship security plan upon upgrade of the MARSEC Level				
Underwater hull and berth/pier screening				

### *SEARCHING THE TERMINAL*

Security sweep of terminal restricted areas



## 2.4.3 Covert Communications



INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

#### **2.4.4 Additional Security Measures**

The security program encompasses many different activities all of which are aimed at providing for the overall safety and security of persons and property onboard the ship. While the intent of this guideline is to present a broad-based approach to security, invariably there will be threats to the ship that will necessitate deviation from this guideline. Accordingly, flexibility in the protective measures may be required to counter specific threats. Where practicable, operators should make the necessary preparatory steps to develop security measures for emerging threats. To assist with this effort, many of the security measures that were implemented in the immediate aftermath of the September 11, 2001 terrorist attack were considered for inclusion in these guidelines. While many of the measures were effective against the threat that existed during that time period, it is unknown as to whether or not they would be applicable during future escalations of the threat level. Accordingly, at the highest level of security, additional security precautions may be individually implemented in coordination with Federal, state, and local authorities. This may include changing port calls, not embarking passengers, or other measures as appropriate.

Through existing regulations in 33 CFR 6.16-3, the COTP retains the authority to issue written requirements for increased security measures to counter a specific threat. This authority may be used to carry out measures such as controlling the movement of ships in the port, establishing security zones, or requiring ship escorts. Similarly, other federal agencies, such as the U.S. Immigration and Naturalization Service (INS), retain the authority to restrict personnel movements on the basis of a specific threat. Accordingly, rather than issue general guidance for ships to carry out these activities at the higher threat levels, these and other security measures may be implemented under the existing authority of the COTP to implement written orders based on specific threats to ship security. Normally, specific measures will only be required at MARSEC III.

#### **2.5 Prevent or Deter Carriage of a Prohibited Weapon, Incendiary, or Explosive**

The general safety and security of the ship and terminal can be accomplished through careful monitoring of all personnel and goods entering and leaving a terminal. The intent of monitoring is to prevent or deter the import of potentially dangerous goods onboard the ship or within the terminal restricted areas. Accordingly, this section addresses the screening and monitoring of passengers, baggage, cargo, and stores.

##### **2.5.1 Prohibited Weapons**

Company security officers should remain aware of the current threat from weapons, incendiaries, and explosives to the ship and terminal. Company security officers should ensure that the screening personnel are adequately trained to screen for prohibited items as

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

per the current threat. [REDACTED]

Unless there is a specific threat to a ship or terminal, the COTP shall not establish a universal definition for prohibited weapons. Rather, this information should be established by company policy.

Companies should establish policies that clearly identify prohibited weapons and the company procedures for securing the weapons.

The company's policy on prohibited weapons should be available to, and incorporated into the training for, security personnel who are responsible for screening personnel, baggage, and stores.

## **2.5.2 Screening Standards**

Reserved.

## **2.5.3 Screening Procedures**

The ship and/or terminal should set up appropriate restricted areas to conduct the screening. It is important that the screening areas be restricted, in order to minimize tampering with the items during and after screening. Note, while landside screening is generally preferred, the screening of smaller items (i.e.: personal effects, cabin baggage, individually packaged stores) need not take place outside the boundaries of the ship provided that screening area onboard the ship is adequately restricted and suspicious items can be removed prior to stowage.

[REDACTED]

[REDACTED]

Anyone refusing to submit to security screening at a point of access shall not be allowed to board a ship.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

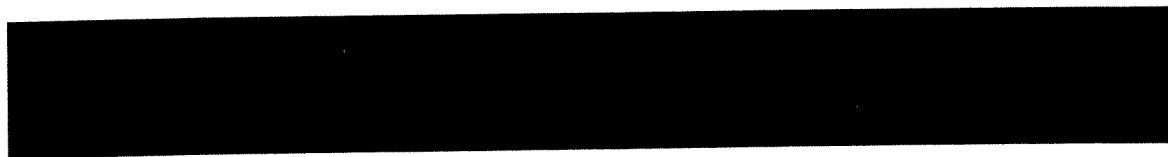
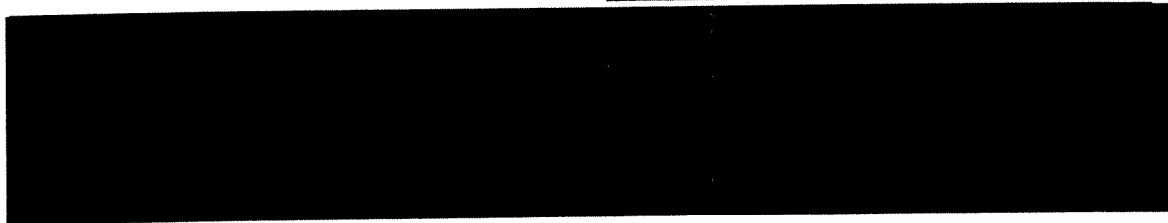
Each person denied entry for refusing to submit to security screening must be identified and reported to the appropriate authorities.

Security equipment should be kept in good working condition and checked/calibrated on a scheduled basis. Records of checks/calibrations should be maintained.

Table 2-3 outlines the recommended frequency of screening for different items commonly brought onboard passenger ships.

**Table 2-3**

<b>MARSEC LEVEL</b>	<b>A</b>	<b>I</b>	<b>II</b>	<b>III</b>
<i>SCREENING FOR WEAPONS, INCENDIARIES, AND EXPLOSIVES</i>				
Individual screenings for weapons (walk through or hand-held metal detectors)				
Screening of checked baggage				
Screening of carry-on items				
Screening of stores and provisions				
Verification of checked baggage against passenger list [or tickets]				



INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

## **2.6 Prevent or Deter Unauthorized Access to the Ship & Restricted Areas**

This section addresses the guidelines for providing terminal and ship physical security, as well as the identification and authorization of personnel.

### **2.6.1 Personnel Security**

Personnel security is comprised of three components: identification cards, background checks, and visitor control.

#### **2.6.1.1 Personnel Identification**

Each passenger ship and passenger terminal operator must establish a system of identification and control of personnel.

This system must be documented in the security plan.

The following procedures should be covered by the plan:

- Identifying each category of persons authorized to be onboard the ship and each person authorized access to a ship or terminal restricted area;
- Identification cards should be issued to each member of the crew or other employee of the ship. Permanent identification cards should contain the cardholder's name, age, height, weight, eye color, expiration date, name of the company that employs the cardholder, and a unique number. Other common forms of identification may also be an acceptable alternative to individual company IDs, provided that the identification cards contain photos or other biometric based information that can be used to accurately identify the individual.
- Providing a temporary identification card to each contractor, vendor, and other visitor authorized access to a restricted area. Once again, other forms of identification may be acceptable if the identification contains a photo.
- Identifying each passenger upon entry into the boarding area. (Terminal security)
- Identifying each passenger authorized to board the ship by comparison against the official passenger list.

Companies should consider combining their process of issuing personnel identification with their process for authorizing personnel access to restricted areas. The combination of the two processes may allow companies to exercise greater control over access to restricted areas through the use of appropriately coded identification badges.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

## **2.6.1.2 Background Checks**

### **2.6.1.2.1 Ship Personnel**

Ship personnel, who are entering the U.S., are screened by U.S. Federal agencies as a part of their normal entry authorization procedures. While federal screening is one tool that will help to identify and deter personnel who may pose a security risk, ship operators should also consider methods of screening, such as pre-employment background checks, in order to promote a reduction in unlawful acts against the industry.

To this end, ship operators should have hiring procedures in place to ensure that the employee backgrounds are vetted, to the extent possible given the range of nationalities, prior to employment. As there are no current regulatory requirements that mandate background checks for ship employees, the specifics of the approach should be set by company policy and may be accomplished through the use of manning agencies, or other equivalent means.

Ship operators should give further consideration to additional employment criteria or more rigorous background checks for employees who are tasked with carrying out ship security responsibilities.

### **2.6.1.2.2 Terminal Personnel**

See section 2.9 regarding background checks on terminal security personnel.

## **2.6.1.3 Visitor Control**

The issue of visitors onboard passenger ships is complex and should not be set in terms of absolute requirements. While unauthorized visitors must not be permitted access to the ship, there are too many variables to define every possible scenario in these guidelines. The company and ship specific security plans will contain far more detail as to the company's visitor policies. To aid with this effort, these guidelines have defined two broad categories of visitors (**Category 1 and Category 2**) and have provided suggested guidance for setting ship specific policies regarding general access control, specific visitor restrictions, and visitor escort requirements.

Category 1 visitors are people visiting the ship for the purposes of the ship's operation or business. This category may include company employees, vendors, repair and service personnel, industry representatives, government officials, agent parties, and invited short-term guests. Further, it should be recognized that certain long-term, frequent vendor representatives may actually be issued company identification cards and thus treated more as employees than as visitors. For this category, the ship operator may permit certain

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

individuals to visit the ship unescorted during heightened MARSEC levels. At the same time, certain persons within this category may require an escort at all times no matter what the MARSEC levels. At the highest MARSEC level, only those Category 1 visitors that have valid company identification issued on the basis of a company background check should be given consideration for unescorted access to the ship.

Category 2 visitors are people visiting the ship for the purposes of recreation or pleasure. They may include customer and employee related visitors such as company or crew family who are visiting but are not on an actual cruise as a passenger, wedding party and guests who may not be passengers on a cruise, invited tour groups such as school classes, or luncheon guests. These persons or groups would normally be escorted at all times. The level of the escort however may vary. For example, crewmembers may escort their own visiting family members. The ability of this category of visitor would be subject to much higher control or restriction depending on the MARSEC level.

Each company must have a visitor control process in place for handling identification, certification, "badging", and escort of all visitors. This process must be comprehensive, but flexible enough to handle the myriad of visitors that the cruise industry deals with on a daily basis. Each company must establish a visitor control policy that documents the specific actions taken for different classes of visitors. This policy does not need to be included in the security plan but should be clearly referenced by the plan. Table 2-4 provides guidance for the setting of company specific policies.

**Table 2-4**

**MARSEC LEVEL**

**A**

**I**

**II**

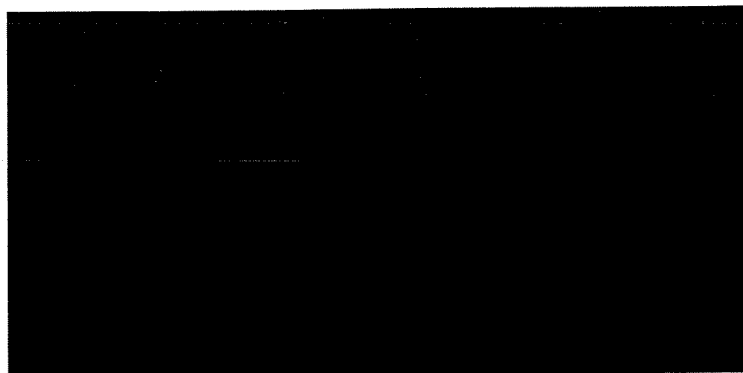
**III**

**ACCESS CONTROL**

Identities checked of ALL personnel entering by production of acceptable photo identification

Identities check of ALL personnel leaving

Each passenger should show a valid ticket, pass, or identification issued by the cruise line to enter the boarding area.



INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION



Increased personnel at access points.

*VISITOR RESTRICTIONS*

Official Visitors Restrictions:  
(Category 1)

Visiting Guests Restrictions:  
(Category 2)

*ESCORT REQUIREMENTS*

Official Visitors: (Category 1)

Customer and Employee Related  
(Category 2)

## **2.6.2 Terminal Physical Security**

The physical security of a terminal can be broken down into restricted areas, barriers, lighting, alarms, communications, and vehicle control. Each one of these areas provides a vital component of the overall physical security of the terminal. The following sections contain guidance on each of these topics.

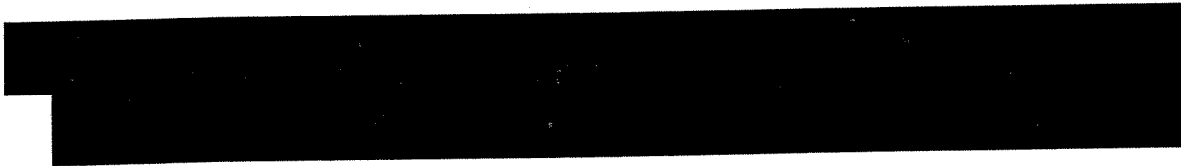
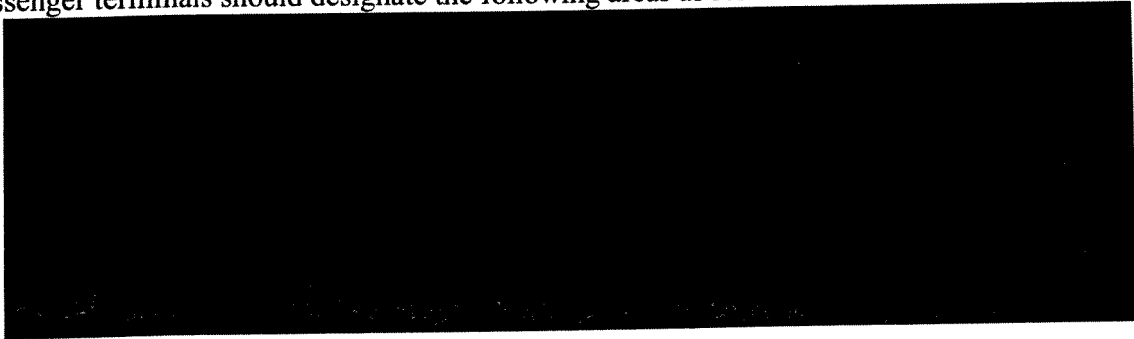
### **2.6.2.1 Restricted Areas**

The establishment of restricted areas helps control and channel access, improves security and increases efficiency by providing degrees of security compatible with the terminal's operational requirements.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

Designated restricted areas should be outlined in the security plan.

Passenger terminals should designate the following areas as restricted areas:



Restricted areas may be further subdivided depending on the degree of restriction or control required to prevent unauthorized access.

#### **2.6.2.2 Barriers**

Barriers and their boundaries, when used between restricted and unrestricted areas in the terminal area, should be clearly defined by walls, fences, environmental design, or other security barriers that are either permanent or temporary in nature.

Barriers should be designed, located, and constructed to –

- Delineate the area protected;
- Create a physical and psychological deterrent so as to prevent the introduction of dangerous substances or devices, and should be of sufficient height and durability to deter unauthorized passage;
- Delay intruders and enable security personnel to detect intruders and, if necessary, apprehend intruders;
- Have a minimum number of openings that provide readily identifiable places for the controlled entry of persons and vehicles into the restricted area;
- Be secure when not watched by security personnel;
- When near roadways, must be reinforced to deter penetration by motor vehicles;
- Be kept clear of trees, bushes, and other obstructions, and
- Barriers may be permanent or temporary in nature.

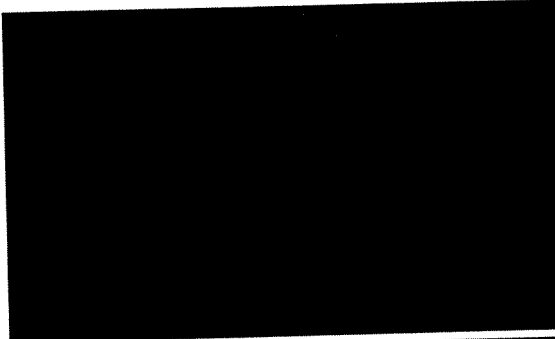

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

The effectiveness of a security fence or barrier against penetration depends to a large extent on the construction employed. The following detail guidelines should be considered when approving/inspecting security barriers:

- Security fence lines should be kept clear of all obstructions.
- The total height of the security fencing should be not less than 2.50 meters.
- Natural barriers such as water, ravines, etc., can sometimes be effectively utilized as part of the control boundary. However, they may require supporting safeguards (i.e.: fencing, security patrols, surveillance, anti-intrusion devices, lighting) especially during high threat periods.
- The roofs of buildings may also provide a possible route for unauthorized access to the restricted area. Safeguards should be taken to prevent such access by these routes.
- Restricted areas partly surrounded by water may require security barriers with sufficient illumination during night hours and, if on navigable waters, frequent and unscheduled patrols by boat or ashore on foot, or both. Illumination of these areas must be of a type and so placed that it does not interfere with safe navigation.

Table 2-5 outlines the required characteristics of physical barriers based on the given threat level.

**Table 2-5**

MARSEC LEVEL	A	I	II	III
<i>PHYSICAL BARRIERS</i>				
Temporary or permanent barriers should be used to maintain segregations between cleared and uncleared passenger and baggage				
Additional safeguards such as fences, walls, patrols, or surveillance should augment buildings and natural barriers.				
Increased manpower at appropriate access points as designated in the security plan.				
				

### 2.6.2.3 Lighting

Passenger terminal operators should provide security lighting between sunset and sunrise.

All external lighting should be located or shielded so that it will not be confused with an aid to navigation and will not interfere with safe navigation.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

Illumination should light each exterior door, gate, fence, pier, wharf, or other point of access to the boarding area for passenger ships.

The following detail guidelines should be considered when approving/inspecting security lighting:

- Facilities should be illuminated to a minimum standard of at least one-foot candle at 1 meter above the ground and should be provided from sunset to sunrise. Dock work areas, waterfront, restricted areas and all access points should have 5 foot candle illumination.
- Updated lighting technology should be used, such as high-pressure sodium, mercury vapor, or metal halide lighting.
- Lighting should be directed downward, away from guards or offices, or navigable waterways and should produce high contrast with few shadows.
- Electrical distribution panels should have secure access or be located in a restricted area.
- The primary system should consist of a series of lights arranged to illuminate a specific area continuously during the hours of darkness or restricted visibility. In some circumstances, it may be preferable to use such lighting systems only in response to an alarm.
- Floodlights may be used to supplement the primary system and may be either portable or fixed.
- Floodlights when used should have sufficient flexibility to permit examination of the barrier under observation and adjacent unlighted areas.
- Controls and switches for security lighting should be located in designated restricted areas.
- Where fences and other barriers are to be illuminated, it is important to ensure that the intensity of illumination is adequate for the purpose.

#### **2.6.2.4 Alarms**

Alarms, when used, should activate an audible or visual alarm when an intrusion is detected. The alarm should sound in a place that is continuously staffed by personnel with security responsibilities.

The following detail guidelines should be considered when approving/inspecting security alarms:

- Intrusion detection systems and alarm devices may be used as a stand-alone security measure. However, at higher MARSEC levels, additional guards and patrols may be necessary to provide greater intrusion protection during periods of increased threat.
- Immediate response capability by guards to an alarm from an intrusion detection system or device is important if its use is to be effective.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

- A wide variety of intrusion detection systems and devices are available for possible use. These systems include those that are sensitive to:
  - Breaking of an electrical circuit;
  - Interruption of a light beam;
  - Sound;
  - Vibration;
  - Motion;
  - Surveillance cameras; or
  - Capacitance change in an electrical field.

### **2.6.2.5 Communications**

Effective communications are a critical component of the terminal security program. Terminal security personnel must be able to communicate from their duty stations with the terminal security officer and the central terminal security station. The central terminal security station must be able to communicate with the security personnel on the ship and the appropriate law enforcement agencies.

A distress signal peculiar to security, indicating a security alert in the terminal area, should be established.

The following detail guidelines should be considered when approving/inspecting communication systems:

- Security and communication system should be tested once per shift and a record of results maintained.
- The terminal should ensure adequate back up/emergency power supply is in place to operate security and communication systems when primary power is interrupted.

### **2.6.2.6 Vehicle Control**

The terminal security officer should develop a policy to control vehicle access to restricted areas. Where possible, establish designated parking areas away from restricted areas. Where practicable, establish exclusionary zones to protect the terminal or ship from vehicle related threats. The measures implemented should be described in the terminal security plan.

The following detail guidelines apply:



- Automobiles approved for entry into passenger terminal facilities should be controlled regarding their destination and parking.
- All vehicles entering or leaving restricted areas should be subject to search by security personnel or competent authority. Signs should be posted advising personnel of this requirement prior to entry.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

- Parking within the passenger terminal facility should be restricted and should be authorized by a strictly enforced gate pass and/or decal system.
- Passes or decals should be color or otherwise coded to further restrict access to authorized times and locations.
- Parking for employees, dockworkers, and visitors should be limited to designated areas that are fenced and generally located outside the boundaries of designated restricted areas (the latter requirement may be linked to the threat level). Temporary permits or passes should be issued to vendors and visitors for parking in designated restricted areas.
- Parking for vehicles authorized on terminal grounds should be restricted largely to port authority, carrier, maintenance, commercial and government vehicles which are essential within the terminal.

Table 2-6 outlines the recommended vehicle restrictions based upon the specified threat level.

**Table 2-6**

MARSEC LEVEL	A	I	II	III
<b>VEHICLE RESTRICTIONS</b>				
Commercial or private vehicles (other than those operated by the terminal) are permitted in restricted areas.				
				

### 2.6.3 Ship Physical Security

The physical security of a ship relies on some of the same principles as the terminal: restricted areas, perimeter security, lighting, alarms, and communications. Each one of these areas provides a vital function in the overall physical security of the ship. The following sections provide guidance on each of these topics.

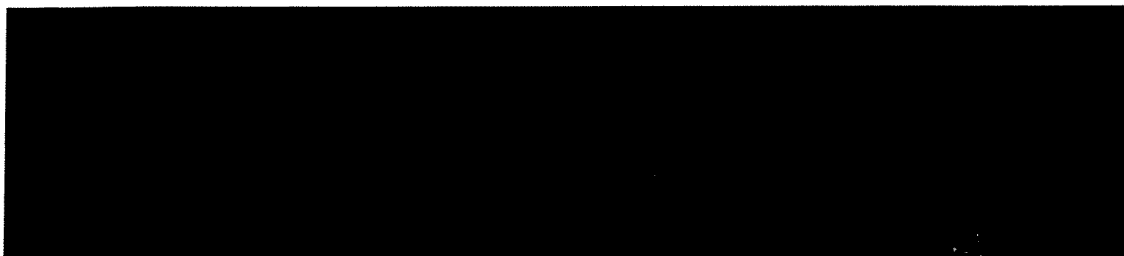
#### 2.6.3.1 Restricted Areas

Designated restricted areas should be outlined in the security plan.

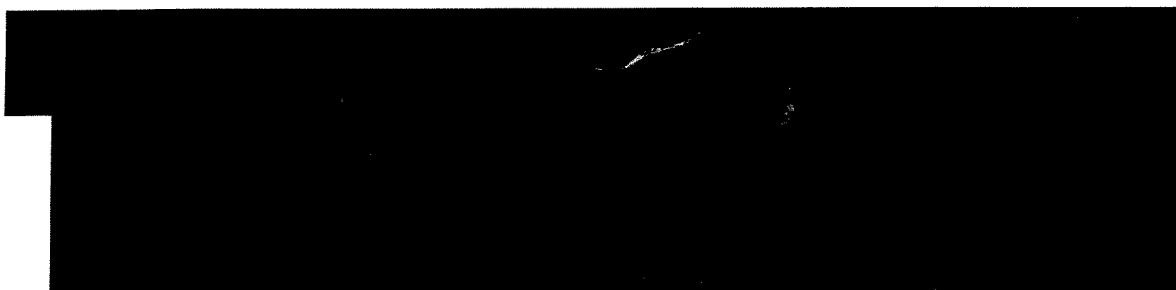
Passenger ships should designate the following areas as restricted areas:



INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION



Each restricted area should be secured and conspicuously marked stating that the area has restricted access.



The master should control the use, number, and distribution of master keys on-board ships. The ship security plan should provide for immediate corrective action in the event of security being compromised by potential misuse or loss of keys.

### 2.6.3.2 Perimeter Security

Table 2-7 outlines the steps that the ship should take to increase perimeter security based on the given security level.

Table 2-7

MARSEC LEVEL	A	I	II	III
<i>SHIP PERIMETER SECURITY</i>				



Boarding ladders/gangways are permitted on the offshore side of ship, provided that the ladders/gangways are continuously attended by security personnel.

All open side ports are manned or otherwise secured to prohibit personnel access\*



INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

Weather-deck access doors to normally unmanned spaces (storerooms, auxiliary machinery rooms, etc.) are locked from outside entry.



### **2.6.3.3 Lighting**

While in port, at anchor, or under way, the ship's deck and over side should be illuminated in periods of darkness and restricted visibility, but not so as to interfere with required navigation lights and safe navigation.

### **2.6.3.4 Alarms**

Alarms, when used to denote unauthorized intrusion into locked or otherwise restricted spaces, should activate an audible or visual alarm when the intrusion is detected.

The alarm should sound in a place that is continuously staffed by personnel with security responsibilities.

### **2.6.3.5 Communication**

The communications section of the plan should specify the kind of communications to use in the event of a breach of security, an unlawful act, or other emergency.

Vessel security personnel should be provided with a means of communications (radio, telephone, intercom, etc.) that enables the personnel to communicate continuously with the ship security officer, the navigational bridge, communication centers, or shore side security personnel.

A distress signal peculiar to security, indicating a security alert, should be established onboard the ship.

### **2.6.4 Waterside Security**

Reserved.

## **2.7 Coordination of Security Activities Between the Terminal and Ship**

The security plan should outline all coordination plans and procedures established with the operator of each passenger terminal. The ship or passenger terminal need not duplicate any security provisions fulfilled by the other.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION



All responsibilities should be clearly outlined in the plan stating who is responsible for which actions on a port-by-port basis.

Copies of the agreements should be contained in the ship security plan.

### **2.7.1 Communication**

Prior to arrival, the terminal should advise the ship of the current threat level at the terminal, any additional security measures that may be in place, and any other pertinent security information.

Communications should be established with each terminal, at which the ship docks, immediately after mooring. This communication should be maintained until the ship departs.

### **2.7.2 Liaison with Law Enforcement**

At all security levels, the ship and terminal security officers should establish closest possible liaison with appropriate law enforcement agencies to ensure that full protective capabilities are deployed in the protection of the ship.

### **2.7.3 Terminal Security at Calling Ports**

Coordination between the ship and terminal/port are essential to ensure that an adequate level of security exists whenever passengers and crew are embarking or disembarking the ship. To this end, a terminal/port security program should be developed and maintained for each calling port regardless of the scope of the operation. These programs should contain an appropriate degree of security based upon local conditions and capabilities. Care should be taken to ensure that security measures are comparable with the anticipated operation based on the number of ships calling and the number of passengers likely to be embarked or disembarked. In general, the security program, and underlying security plan, for calling ports will be less than that which is required for terminals where passengers, baggage, and stores are loaded or off-loaded.

The following comments provide guidance for tailoring the general security program guidelines to calling ports:

- Prevent or Deter Carriage Aboard of Prohibited Weapons, Incendiary, or Explosive Device: Screening of passengers, hand-carried items, and similar packaged supplies may be conducted onboard the ship. In accordance with the threat, security personnel should screen large items, such as vehicles or palletized supplies at the entrance to shore-side restricted areas.
- Prevent or Deter Unauthorized Access to Restricted Areas: A restricted area should be established on the shore side in the area where personnel and garbage/supplies will be off-loaded or loaded. Access to and from the restricted area should be controlled,

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

as appropriate, for the given threat level. At lower threat levels, access controls should be focused on restricting access or screening large vehicles (i.e. trucks). At higher threat levels the restricted area may be expanded in size, but should also have increased access control restrictions for smaller vehicles and personnel.

- Safety and Security of Persons and Property: The Company Security Officer should establish liaisons with local law enforcement assets to identify resources and procedures for implementing additional security measures.

## **2.8 Training for Security Personnel**

### **2.8.1 General**

A continuous and thorough training program should support measures taken to safeguard the security of passengers and crews onboard ships. Basic guidance for development of security training and education is given in the following paragraphs.

### **2.8.2 Criteria**

Security training should meet the following criteria:

- Be comprehensive
- Have a clearly defined objective, i.e. the attainment of an established minimum standard of proficiency, knowledge, and skill to be demonstrated by each individual as established by the company security plan.

### **2.8.3 Terminal Security Personnel**

Proper training in all security procedures is critical to the functionality of the overall security program. The following sections highlight the key aspects of terminal security training programs.

#### **2.8.3.1 Terminal Security officer and appropriate staff**

The terminal security officer and appropriate terminal staff should have knowledge and, as necessary, receive training in some or all of 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;
- Ship 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;
- Dangerous substances and devices, and how to recognize them;
- Ship and local port operations and conditions; and
- Security devices and systems.

### **2.8.3.2 Security inspection, control, and screening personnel**

Instruction and, where appropriate, training for persons assigned to conduct inspection, control and monitoring at a terminal should take into consideration, as appropriate:

- Responsibilities under the terminal plan or ship security plan;
- Inspection, control, and monitoring regulations or policies and pertinent laws;
- Detection and identification of prohibited weapons, incendiary, or explosive devices;
- Operation and testing of security equipment;
- Manual search methods of persons, baggage, cargo, and ship's stores;
- Emergency procedures;
- Recognition of characteristics and behavioral patterns of persons who are likely to commit unlawful acts;
- Human relations techniques; and
- Techniques used to circumvent security measures.

### **2.8.3.3 Guards**

Terminal guards who are assigned either to specific fixed locations or to patrols for the purpose of preventing unauthorized access to areas should receive a general briefing on the training subjects recommended for the terminal security officer. Initial and subsequent training should emphasize techniques for:

- Entry control;
- Patrols, observation, and communications;
- Inspection, identification, and reporting;
- Person, building, and vehicle searches;
- Apprehension of suspects;
- Self-defense;
- Recognizing dangerous substances and devices;
- Human relations; and
- First aid.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

## **2.8.4 Ship Security Personnel**

Proper training in all security procedures is critical to the functionality of the overall security program. Security training should be appropriate for the duties assigned to the person. The following sections highlight the key aspects of security training programs.

### **2.8.4.1 Company Security Officer and Staff**

The Company Security Officer and appropriate staff should have knowledge and, as necessary, receive training in some or all of 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;
- Ship 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;
- Dangerous substances and devices, and how to recognize them;
- Ship and local port operations and conditions; and
- Security devices and systems.

### **2.8.4.2 Ship Security Officer**

The ship security officer should have adequate knowledge of and, if necessary, training in the following, as appropriate:

- The ship security plan and related emergency procedures;
- The layout of the ship;
- The assessment of the risk, threat, and vulnerability;
- Methods of conducting security inspections;
- Techniques used to circumvent security measures;
- Operation of technical aids to security, if used;
- Recognition of characteristics and behavioral patterns of persons who may be likely to commit unlawful acts;
- The detection and recognition of dangerous substances and devices;
- Port and ship operations; and
- Methods of physical searches of persons and their baggage.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

### **2.8.4.3 Inspection, Control and Monitoring Personnel**

Instruction and training, as appropriate, for persons assigned to conduct inspection, control and monitoring onboard ships should take into consideration, as appropriate, the following:

- Responsibilities under the terminal or ship security plan;
- Inspection, control, and monitoring regulations or policies and pertinent laws;
- Detection and identification of prohibited weapons, incendiary, or explosive devices;
- Operation and testing of security equipment, if used;
- Physical search methods of persons, baggage, cargo, and ship's stores;
- Emergency procedures;
- Recognition of characteristics and behavioral patterns of persons who are likely to commit unlawful acts;
- Human relations techniques; and
- Techniques used to circumvent security measures.

### **2.8.4.4 Ship's Crew**

Crew members having specific security duties should know their responsibilities for ship security as described in the ship security plan and should have sufficient knowledge and ability to perform their assigned duties. All crew should receive sufficient training to recognize and know how to report suspicious activities or occurrences.

### **2.8.5 Law Enforcement Personnel**

Appropriate law enforcement personnel, when not directly involved in or responsible for terminal security, should receive a general briefing to become familiar with port and ship operations and the training of terminal and ship operator security personnel. They should also be orientated regarding inspection, control, and monitoring and the security plans.

### **2.8.6 Security Drills and Exercises**

Reserved.

## **2.9 Pre-Hiring Evaluation of All Terminal Security Personnel (Terminal Only)**

33 CFR 128.200(a)(6) requires company or terminal security officers to conduct pre-employment evaluations on all terminal security personnel as a condition of hiring.

The pre-employment evaluations should consist of a criminal background check for unlawful acts as defined earlier by this guide.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

Each company should have documented procedures that describe their process for conducting background checks. These procedures need not be contained in the terminal security plan, but should be referenced by the terminal security plan.

This requirement should be applicable to all companies who employ security personnel in the terminal, irrespective of whether they are employed by the ship operator, the terminal operator, or another party.

Personnel who are not performing security functions, but who are working in restricted areas should have similar pre-employment evaluations, or should be appropriately screened to ensure that they are not transporting prohibited items into the restricted area.

### **3 Reports of Security Violations**

Passenger ship and terminal operators must report each breach of security, unlawful act, or threat of an unlawful act that threatens the security of passengers and crews onboard a ship or terminal.

Each company should maintain a file of security reports for a period of two years.

#### **3.1 Ship Security Violation Reports**

All ships to which 33 CFR 120 applies:

Either the company or ship security officer must report each breach of security, unlawful act, or threat of an unlawful act against any of your passenger ships to which this part applies, or against any person onboard it, that occurs in a place subject to the jurisdiction of the United States.

Either company or the ship security officer must file a written report of the incident, using the form "Report on an Unlawful Act," contained in IMO MSC Circular 443. The incident must be reported to both the COTP and to the local office of the Federal Bureau of Investigation (FBI). A copy of the report should be forwarded to Commandant (G-MP), U.S. Coast Guard Headquarters, 2100 Second Street SW., Washington, DC 20593-0001.

If the incident occurs while the vessel is underway in waters that are subject to the jurisdiction of the U.S. (U.S. Exclusive Economic Zone), then the incident should be reported to the COTP and the FBI at the vessel's next U.S. port call. As an alternative, you may file the report initially with Commandant (G-MP) by fax at (202) 267-4700.

Additional reporting requirements for U.S. Flag ships to which 33 CFR 120 applies: In addition, for U.S. Flag ships, each such incident that occurs in a place outside the jurisdiction

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

### REPORT ON AN UNLAWFUL ACT

DATE: \_\_\_\_\_

1. DESCRIPTION OF SHIP OR PORT AREA:

NAME OF SHIP \_\_\_\_\_

FLAG \_\_\_\_\_

MASTER \_\_\_\_\_

TERMINAL SECURITY OFFICER \_\_\_\_\_

2. BRIEF DESCRIPTION OF INCIDENT OR THREAT:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

DATE, TIME, AND PLACE OF INCIDENT OR THREAT \_\_\_\_\_

3. NUMBER OF ALLEGED OFFENDERS:

PASSENGER \_\_\_\_\_; CREW \_\_\_\_\_; OTHER \_\_\_\_\_.

4. METHOD UTILIZED TO INTRODUCE DANGEROUS SUBSTANCES OR DEVICES INTO THE TERMINAL OR SHIP:

PERSONS \_\_\_\_\_; BAGGAGE \_\_\_\_\_; CARGO \_\_\_\_\_; SHIP STORES \_\_\_\_\_; OTHER \_\_\_\_\_.

5. TYPE OF DANGEROUS SUBSTANCES OR DEVICES USED, WITH FULL DESCRIPTION:

WEAPON -EXPLOSIVES -OTHER

6. a) WHERE WERE THE ITEMS DESCRIBED IN SECTION 5 ABOVE CONCEALED, IF KNOWN?

\_\_\_\_\_

b) HOW WERE THE ITEMS DESCRIBED IN SECTION 5 ABOVE USED AND WHERE?

\_\_\_\_\_

c) HOW WERE THE SECURITY MEASURES CIRCUMVENTED?

\_\_\_\_\_

7. WHAT MEASURES AND PROCEDURES ARE RECOMMENDED TO PREVENT RECURRENCE OF A SIMILAR EVENT?

\_\_\_\_\_

8. OTHER PERTINENT DETAILS:

\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_  
\_\_\_\_\_

Figure 1

of the United States must be reported to the hotline of the National Response Center of the Department of Transportation at 1-800-424-8802, or, 202-267-2675.

### **3.2 Terminal Security Violation Reports**

Either the terminal operator or the terminal security officer must report (see form on following page) each breach of security, unlawful act, or threat of an unlawful act against the terminal, a passenger ship subject to 33 CFR part 120 moored at that terminal, or any person aboard the terminal or ship, to the COTP, to the local office of the FBI, and to the local police agency having jurisdiction over the terminal.

### **3.3 Standard Report Form**

Figure 1 is a copy of the standard report form. Other report forms may be acceptable provided that the forms include the information shown in Figure 1.

## **4 Security Plan**

The MSC and COTP will consider the following guidelines when reviewing security plans. The emphasis of the regulations is on developing a coordinated security program to protect the ship and personnel onboard the ship. It is essential that ships, terminals, and law enforcement agencies agree and understand the security program and be willing partners in its operation.

### **4.1 Security Plan Details**

The security plan should adequately describe, or reference, the personnel and procedural details of the security program. The following sections provide guidelines as to the type of information that should be included in the security plan and the responsibilities of the company security officer, or designated representative, for conducting periodic assessments of, and amendments to, the security plan.

#### **4.1.1 Security Program Personnel and Procedures**

The plan should describe, or reference, procedures for all aspects of the security program discussed in section 2 of this guide. Specifically, the plan should:

- Describe activities to prevent or deter unauthorized access to the ship/terminal and its restricted areas;
- Describe activities to prevent or deter the introduction of prohibited weapons, incendiaries, and explosives aboard the ship/terminal;
- Describe activities to encourage vigilance, as well as general awareness of security, onboard the ship/within the passenger terminal;
- Designate, by name, a security officer for the ship/terminal and outline the duties and responsibilities of the security officer;

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION



- Provide adequate training to members of the crew/terminal personnel for security aboard the ship/terminal;
- Coordinate responsibilities for security between the ship operator and the operator of each terminal at which the ship embarks and disembarks passengers (Copies of the agreements should be contained in the security plan.);
- Document the standard operating procedures, including watch-standing, and standard response procedures (e.g. bomb threat, unauthorized person, unauthorized ship/vehicle, loss of power/lighting, suspicious activity, mail handling, suspicious package), and incident reporting procedures;
- Provide information to members of the crew/terminal personnel and to law-enforcement personnel, in case of an incident affecting security;
- Discuss procedures for making amendments to the plan to address any known deficiencies (All amendments must bear the notation "Examined by the Coast Guard" along with the date of examination); and
- Discuss procedures to restrict the distribution, disclosure, and availability of information contained in the plan to those persons with an operational need to know.

#### **4.1.2 Security Survey**

Since each plan must be unique and specific to each ship or terminal, the security survey forms the basis for the development and amendment of the security plan. Furthermore, through regular updates, the security survey also provides the opportunity for the owners to monitor compliance with the plan and make amendments as necessary.

All reported violations (see section 3), which occurred since the previous survey, should be provided to the surveyor for consideration.

Security surveys must be updated on a periodic basis. Surveys should be updated at least annually, but may be updated more frequently, as necessary.

##### **4.1.2.1 Periodic Ship Security Surveys**

The ship security survey is broken down into three parts: an assessment, an on-scene security survey, and a ship security report.

###### **4.1.2.1.1 Assessment**

Prior to commencing the ship security survey, the company security officer should take advantage of such information as is available to him/her on the assessment of threat for the ports at which the ship will call and about the port facility and security measures. The security officer should study previous reports on similar security needs.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

Where feasible, the company security officer should meet with appropriate persons on the ship and in the port facilities to discuss the purpose and methodology of the survey.

The company security officer should obtain and record the information required to conduct a vulnerability assessment, including:

- 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 the 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.

#### ***4.1.2.1.2 On-scene security survey***

The company security officer should examine and evaluate the methods and procedures used to control access to ships, including:

- Inspection, control and monitoring of persons and carry-on articles; and
- Inspection, control and monitoring of cargo, ship's stores, and baggage.

The company security officer should examine each identified point of access, including open weather decks, and evaluate its potential for use by individuals who might be engaged in unlawful acts. This includes individuals having legitimate access as well as those who seek to obtain unauthorized entry.

The company security officer should examine and evaluate existing security measures, procedures and operations, under both emergency and routine conditions, including:

- Established security procedures;
- Response procedures to fire or other emergency conditions with regard to maintaining security;
- The level of supervision of the ship's crew, vendors, repair technicians, dock workers, etc.;
- The frequency and effectiveness of security patrols;
- The security key control system;
- Security communications systems and procedures; and
- Security doors, barriers, and lighting.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

#### ***4.1.2.1.3 Ship Security Survey Report***

This report should include the following items:

- The date of the survey;
- Names of the owner and operator of the ship;
- The names, business addresses, and telephone numbers of the ship, security officer; and company;
- A description of the ship that includes general layout of the ship;
- Location of restricted areas;
- The open deck arrangement including the height of the deck above the water;
- Emergency and standby equipment available to maintain essential services;
- Number of ship's crew.

#### ***4.1.2.2 Periodic Terminal Security Survey***

The terminal security survey contains the same elements as the ship security survey: an assessment, an on-scene security survey, and a terminal security report.

##### ***4.1.2.2.1 Assessment***

Prior to commencing the survey the terminal security officer should obtain current information on the assessment of threat for the locality and should be knowledgeable about the terminal and type of ships calling at the port. The security officer should study previous reports on similar security needs and know the general layout and nature of the operations conducted.

The terminal security officer should meet with appropriate representatives of the terminal, of the operator, or of both of them, to discuss the purpose and methodology of the survey.

The terminal security officer should obtain and record the information required to conduct a vulnerability assessment, including:

- The general layout of the terminal and terminal including topography, building locations, etc.;
- Areas and structures in the vicinity of the terminal such as fuel storage depots, bridges, locks, etc.;
- The degree of dependence on essential services, such as electric power, communications, etc.;
- Stand-by equipment to assure continuity of essential services;
- Locations and functions of each actual or potential access point;
- Numerical strength, reliability and function of staff, permanent labor and temporary labor forces;

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

- The details of existing security measures and procedures, including inspection, control and monitoring procedures, identification documents, access control procedures, fencing, lighting, fire hazards, storm drains, etc.;
- The equipment in use for protection of passengers, crews, and terminal personnel;
- All vehicle traffic or services which enter the terminal; and
- Availability of other personnel in an emergency.

#### ***4.1.2.2 On-scene Security Survey***

The terminal security officer should examine and evaluate the methods and procedures used to control access to ships and restricted areas in the terminal, including:

- Inspection, control and monitoring of persons, and carry-on articles;
- Inspection, control and monitoring of cargo, ship stores, and baggage; and
- Safeguarding cargo, ship stores, and baggage held in storage within the terminal.

The terminal security officer should examine each identified point of access to ships and restricted areas in the terminal and evaluate its potential for use by individuals who might be engaged in unlawful acts. This includes persons having legitimate access as well as those who seek to obtain unauthorized entry.

The terminal security officer should examine and evaluate existing security measures, procedures and operations under both emergency and routine conditions, including:

- Established safety procedures;
- Restrictions or limitations on vehicle access to the terminal;
- Access of fire and emergency vehicles to restricted areas and availability of parking and marshalling areas;
- The level of supervision of personnel;
- The frequency and effectiveness of patrols by security personnel;
- The security key control system;
- Security communications, systems and procedures; and
- Security barriers and lighting.

#### ***4.1.2.2.3 Terminal Survey Report***

This report should include the following items:

- The date of the survey;
- Names of the owner and operator of the terminal;
- The name, business address, and telephone number of the terminal security officer;
- A description of the terminal that includes general layout and access points;
- Intensity of security lighting;
- Restricted areas;
- Emergency equipment;

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

- Location of firearms and ammunition at the terminal;
- List of persons authorized to carry firearms and type of firearms carried;
- Number of security personnel employed; and
- Number of other employees normally at the terminal when a ship embarks and disembarks passengers.

## **4.2 Security Plan Review Requirements**

In accordance with 33 CFR 120.300 and 33 CFR 128.300, the Coast Guard must examine the security plans and their amendments for passenger ships and terminals.

Passenger ship security plans are reviewed by the MSC.

Passenger terminal security plans are reviewed by the cognizant COTP.

These plans are exempt from disclosure under the Freedom of Information Act (FOIA) and are not releasable to the public.

Passenger ships should only embark passengers from or disembark passengers to terminals that:

- Hold an examined terminal security plan; or
- Hold a letter from the COTP stating normal operations may continue until plan review is completed.

**Enforcement:** The COTP may make use of enforcement tools such as Letters of Warning, Notices of Violation, and COTP Orders to gain compliance with 33 CFR Parts 120 and 128. The COTP may take into consideration compliance with these guidelines in making enforcement determinations. They may even use civil and criminal penalties authorized under the provisions of 33 U.S.C. 1221.

**Right of Appeal:** Any person directly affected by a decision or action taken by the MSC may appeal that action or decision to the Assistant Commandant for Marine Safety, Security, and Environmental Protection Commandant (G-MS) according to the procedures in 46 CFR 1.03-15. Any person directly affected by a decision or action taken by the COTP may appeal that action or decision to the cognizant District Commander also according to the procedures in 46 CFR 1.03-15; and may appeal the District Commander's decision to the Commandant according to the procedures in 46 CFR 1.03-25.

### **4.2.1 Ship Security Plan Review**

Ship operators are responsible for preparing and holding a security plan that meets the requirements of 33 CFR 120.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

#### **4.2.1.1 Initial Review**

The operator of the ship must submit at least two copies of the plan to the MSC at least 60 days before embarking passengers on any voyages that subject the ship to this regulation. [Note: In some cases you may submit terminal security plans, see section 4.2.2 for additional guidance.]

If the MSC is unable to complete the review within 30 days after it receives a ship security plan, it will issue you a letter stating that the ship security plan is currently under review. The letter will grant permission for ship operations to continue until the examination is completed. The MSC then has an additional 90 days to complete an examination and provide a response. The MSC has a total of 120 days after receiving the plan to complete an examination and provide a response.

If the MSC finds that the plan meets the requirements of reference (a), both copies will be marked "Examined by the Coast Guard". One copy will be returned to you, and the second copy will be forwarded to Commandant (G-MP).

If the MSC finds that the ship security plan does not meet the requirements of reference (a), the plan will be returned to you with an explanation of why it does not meet them. The second copy of the plan, along with a copy of the response, will be retained by the MSC. Except in emergencies, the MSC will allow you 60 days to comply with the regulations.

#### **4.2.1.2 Security Plan Amendments**

Each proposed amendment to the plan initiated by you, including changes to the enclosures, should be submitted to the MSC for review at least 30 days before the amendment is to take effect. The MSC has the discretion to allow a shorter period of time. Commandant (G-MP) should retain copies of accepted amendments.

The most recent ship security survey report should be referenced, and available for review, to support amendments to the security plan. Security reports need not be made available to support administrative amendments (i.e. changes to contact information) to the security plan.

#### **4.2.2 Terminal Security Plan**

Passenger terminal security plans are reviewed by the cognizant COTP. Subject to these guidelines, the COTP is responsible for establishing the procedures for conducting the initial review of the terminal security plan.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

#### 4.2.2.1 Initial Review

Since the regulations were implemented, many COTPs have found that not all terminals share equally in the process of security plan development. Many terminals that embark or disembark passengers are not solely in the business of passenger service and view their responsibilities as less than the ship's responsibilities.

Because of contractual differences, the ship will often assume more of the security burden than the terminal. Therefore, flexibility in determining or coordinating plan development is essential to ensure an adequate degree of security exists regardless of who submits the security plan.

The bottom line is that the terminal security plan should contain sufficient local resources and contacts to provide security assets as needed for all MARSEC Levels and that the ship, terminal, and law enforcement authorities are all involved in the plan to ensure its success when activated.

The ship owner or operator should submit a terminal security plan if there is an agreement between the owner or operator of the passenger terminal and the owner or operator of the ship that the ship will submit the required plan.

The ship may submit the terminal security plan to the cognizant COTP when any of the following conditions exist:

- When the owner or operator of the ship has exclusive use of a pier and terminal building immediately adjacent to the pier and has complete control of the area.
- When there is no terminal.\*
- When passengers embark and or disembark and no baggage or stores are loaded or offloaded.\*

(\*) With the permission of the cognizant COTP, an annex to the ship's security plan may be used to document the terminal security program. This annex should address the security guidelines for calling ports, as discussed in section 2.7.3 of this guide.

The terminal owner or operator should submit the terminal security plan when any of the following conditions exist:

- When there is an agreement with the owner or operator of a passenger ship that the owner or operator of the terminal will submit the required plan.
- When no security agreement exists; or
  - At least one ship other than a passenger ship uses the terminal;
  - More than one passenger ship uses the terminal; and
  - The terminal loads or offloads baggage or stores.

INFORMATION REDACTED UNDER 49 CFR PART 1520 AS SENSITIVE SECURITY INFORMATION

#### **4.2.2.2 Security Plan Amendments**

Each proposed amendment to the plan you initiate, including changes to enclosures, must be submitted to the COTP for review at least 30 days before the amendment is to take effect. The COTP has the discretion to allow a shorter period of time. Copies of accepted amendments should be retained by the COTP.

The most recent terminal security survey report should be referenced, and available for review, to support amendments to the security plan. Security reports need not be made available to support administrative amendments (i.e. changes to contact information) to the security plan.

#### **4.2.3 Security Plan Assessments**

The COTP should ensure that the security plan reflects the ship/terminal security program and procedures that are actually in place by conducting periodic onsite assessments. Onsite assessments should occur at least once per year, but may occur more frequently as necessary. The port physical security checklist [enclosure 2-3 to the Marine Safety Manual Volume VII] is not required. Further, this process supersedes the annual reporting requirement established by section 2-C.1.b. "Physical Security Assessments" of volume VII of the Marine Safety Manual. As with all other types of boardings or inspections, coordination with the terminal senior personnel is absolutely necessary. The assessment should:

- Verify the presence of an examined security plan;
- Review reports of unlawful acts;
- Observe the security practices actually in place; and
- Observe drills/exercises.\*

\*Note: Guidance for this activity is reserved pending development of section 2.8.6 of this document.

No assessment will be made without the knowledge of the Company Security Officer or designated representative.



### **Review Checklist for a Vessel/Terminal Security Plan**

In order to provide interim approval of a vessel/terminal security plan amended pursuant to this NVIC, the Coast Guard reviewer will need to confirm –

1. The plan is amended to reflect the performance standards in the following tables:
  - Table 2-1 Information
  - Table 2-2 Searching the Ship/Terminal
  - Table 2-3 Screening for Weapons, Incendiaries, and Explosives
  - Table 2-4 Access Control
  - Table 2-5 Physical Barriers
  - Table 2-6 Vehicle Restrictions
  - Table 2-7 Ship Perimeter Security
2. Additionally, each plan should address the following:
  - Identification of the personnel and procedures for searching the ship/terminal.
  - A system of identifying the equipment, personnel, and procedures that will be used to conduct screening activities.
  - Designate restricted areas and identify the means to be used in controlling access to those areas.
  - A system of identification and control of personnel.
  - A visitor control process for handling identification, certification, badges, and escort of all visitors.
  - Terminal plans that include a policy to control vehicle access to restricted areas.
  - Details regarding training for security personnel.

