

Code. The enforcement of these additional standards through the port State control program contributed to a further reduction of substandard vessels visiting the U.S. At the inception of the port State control program, USCG efforts relating to maritime security mostly involved foreign cruise vessels and certain waterfront facilities. The events of September 11, 2001, however, underscored the need for increased security efforts including evaluating, examining, and controlling visiting vessels. The USCG worked diligently since 9/11 to develop comprehensive national and international security standards. In December 2002, the International Maritime Organization (IMO) adopted amendments to the International Convention of Safety of Life at Sea (SOLAS): Chapter XI-2, "Special Measures to Enhance Maritime Security," and the International Ship and Port Facility Security (ISPS) Code. In October 2003, the USCG published six Final Rules in title 33 of the Code of Federal Regulations (CFR), Subchapter H, which were issued under the authority of the Maritime Transportation Security Act of 2002 (MTSA).

5. **DISCUSSION:** The USCG will enforce applicable requirements of SOLAS Chapter XI-2, the ISPS Code, and the maritime security regulations authorized by MTSA for all foreign vessels subject to SOLAS and all foreign commercial vessels greater than 100 GRT that enter U.S. ports. In order to provide a comprehensive framework for these maritime security standards, these standards are seamlessly integrated into the existing port State control program. The procedures and policies offered herein provide expanded program guidelines for targeting vessels for examination, conducting vessel examinations, controlling substandard vessels, and tracking and reporting results of vessel examinations.

6. **IMPLEMENTATION:** Ship security performance is paramount to maritime security implementation. Since a ship is required to have an approved security plan in place, the provisions of the plan should be fully implemented—and its implementation, including applicable requirements of ISPS Code Part A, taking into consideration the relevant guidance of ISPS Code Part B, should be apparent to the port State control officer (PSCO). The PSCO should determine if a vessel is complying to its plan and other maritime security requirements through observation, asking questions, and reviewing security records. If there are clear grounds that the vessel does not meet the applicable maritime security requirements, the COTP should impose appropriate control and/or enforcement actions. These may include inspection, delay, or detention of the ship; restriction of ship operation; expulsion of the ship from port; and/or lesser administrative or corrective measures. If the only means to verify or rectify the non-compliance is to review the relevant portions of the ship security plan, the PSCO must obtain permission from the Master or the flag State as described in Paragraph 9.8.1 of ISPS Code, Part A before reviewing the plan. Further guidance on determining whether a vessel meets applicable maritime security requirements is provided in Paragraphs C.5.d and C.6.d of Enclosure (3) to this NVIC. If, during inspection of the ship, the COTP concludes, for example, the provisions of the approved ship security related to screening of personnel are satisfactory, but the ship and its crew are not implementing these provisions, the COTP shall take appropriate control and enforcement actions. Furthermore, if the COTP concludes that provisions of the ship security plan relating to screening of personnel do not meet the requirements of ISPS Code Part A, taking into consideration the recommendations of ISPS Code Part B, the COTP should also take appropriate control and enforcement actions. The implementation policy herein includes four key pieces: Risk-based targeting; reporting and

notification; boarding procedures; and control and enforcement procedures. Risk-based targeting, discussed in Enclosure (1), focuses on three issues: vessel security risk; risk of vessel noncompliance with international and national maritime security standards; and risk of vessel noncompliance with international and maritime safety and environmental standards. Enclosure (2) addresses tracking and reporting the results of vessel examinations. Boarding procedures, provided in Enclosure (3), discuss law enforcement security boardings of foreign vessels and safety and security compliance examinations for convention and non-convention foreign vessels. Enclosure (4) provides control and enforcement procedures for substandard vessels. To meet the responsibilities discussed herein, Coast Guard Marine Safety and Operations communities need to work in concert with industry, State and local governments, and volunteer agencies to focus on preventing vessel security and safety-related incidents. In addition, units should take note of the following when applying the guidance of this circular:

- a. The Maritime Law Enforcement Manual (MLEM), COMDTINST M16247.1 (series) should be used in tandem with this NVIC when performing security boardings. The MLEM gives policy guidance for execution of the USCG's law enforcement mission and provisions related to armed security boardings, and should be adhered to accordingly.
- b. The Marine Safety Manual (MSM), Volume II (Materiel Inspection) , COMDTINST M16000.7A should be used in tandem with this circular when performing compliance examinations. When the MSM guidance conflicts with the guidance provided herein, the guidance in this circular takes precedence over the MSM. In cases of apparent policy conflict between this NVIC and the MSM, Commandant (G-MOC) should be notified. It should be noted that the guidance in the MSM pertaining to port State control is scheduled for update and the guidance herein will be included in this update.
- c. Operational units should review the procedures described herein and incorporate them as appropriate into unit plans and activities.

7. INFORMATION SECURITY.

- a. Security assessments, security plans and their amendments contain information that, if released to the general public, would compromise the safety or security of the port and its users. This information is known as sensitive security information (SSI), and the Transportation Security Administration (TSA) governs SSI through 49 CFR 1520, titled "Protection of Sensitive Security Information." These regulations allow the Coast Guard to maintain national security by sharing unclassified information with various vessel and facility personnel without releasing SSI to the public. Vessel and facility owners and operators must follow procedures stated in the 49 CFR 1520 for the marking, storing, distributing and destroying of SSI material, which includes many documents that discuss screening processes and detection procedures.
- b. Under these regulations, only persons with a "need to know," as defined in 49 CFR 1520.11, will have access to security assessments, plans and amendments. Vessel and facility owners or operators must determine which of their employees need to know which provisions of the

security plans and assessments, then the owners and operators must restrict dissemination of these documents accordingly. To ensure that access is restricted to only authorized personnel, SSI material will not to be disclosed under the Freedom of Information Act (FOIA) under almost all circumstances.

- c. When SSI is released to unauthorized persons, a report must be filed with the Department of Homeland Security. Such unauthorized release is grounds for a civil penalty and other enforcement or corrective action.
8. **DISCLAIMER.** While the guidance contained in this document may assist the industry, the public, the USCG, and other Federal and State regulators in applying statutory and regulatory requirements, this guidance is not a substitute for applicable legal requirements, nor is it in itself a rule. Thus, it is not intended to nor does it impose legally binding requirements on any party, including the USCG, other Federal agencies, the States, or the regulated community.
9. **CHANGES.** This NVIC will be posted on the web at www.uscg.mil/hq/g-m/nvic/index00.htm. Changes to this circular will be issued as necessary. Time-sensitive amendments will be issued as “urgent change” messages by ALDIST/ALCOAST and posted on the website for the benefit of industry, pending their inclusion to the next change to this circular. Suggestions for improvement of this circular should be submitted in writing to Commandant (G-MOC).
10. **FORMS AVAILABILITY.** Forms can be retrieved at <http://cgweb.comdt.uscg.mil/g-mp/g-mp.htm> and reproduced locally.



THOMAS H. GILMOUR
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Marine Safety, Security
And Environmental Protection

- Encl:
- (1) Risk-Based Targeting for all Vessels
 - (2) Reporting and Notification Procedures
 - (3) Boarding Procedures
 - (4) PSC Enforcement and Control Procedures and Appendix A Examples of Detainable Deficiencies for Security and Safety
 - (5) Glossary
 - (6) CG-840 “Foreign Vessel Exam Book for MTSA/ISPS Code Compliance”

Table of Contents

Coast Guard Port State Control Targeting and Boarding Policy for Vessel Security and Safety

Enclosure 1—Risk-Based Targeting for All Vessels

Introduction.....	3
A. Action – Using the Matrices	3
1. Targeting Philosophy – Security Compliance	4
2. Targeting Philosophy – Safety and Environmental Protection Compliance	4
Figure 1-1: Boarding Decision-Making Process for Each Vessel Arrival.....	6
B. Compliance Targeting Instructions (Step I & Step II)	7
1. Step I: <i>ISPS/MTSA Security Compliance Targeting Matrix</i>	7
2. Step II: <i>PSC Safety and Environmental Protection Compliance Targeting Matrix</i>	10
3. <i>Compliance Verification Examination Matrices</i>	13
C. Boarding Decision and Location (Step III).....	14
1. ISPS I and Priority I (PI) Boardings	15
2. ISPS II and Priority II (PII) Boardings	15
D. Targeting Factor Criteria.....	15
1. Security Compliance Targeting Criteria	15
2. Safety and Environmental Protection Compliance Targeting Criteria	17
Table 1-1: Detention Ratios and Point Assignments	17

Enclosure 2—Reporting and Notification Procedures

Introduction.....	3
A. Security and Safety-Related Detentions, Unit Responsibilities.....	3
1. Flag State Notification	3
2. USCG Headquarters/Area/District Notification	4
3. Classification Society/Recognized Organization/Recognized Security Organization Notification	4
4. Ship Management Notification	5
B. Security and Safety-Related Detentions, USCG Headquarters Responsibilities.....	5
1. Ship Management Notification	5
2. International Maritime Organization Notification	5
C. Table 2-1: IMO Detention Notification Responsibility Chart	6
D. Documentation.....	7
1. Detentions	7
2. Deficiency Compliance Dates.....	7

3.	Deficiency Format	7
----	-------------------------	---

Enclosure 3—Boarding Procedures

Introduction.....	3
1. Types of Boarding Exams.....	3
2. Authority	4
A. Table 3-1: Boarding Decision/Boarding Location Reference Table for Vessels Arriving or In a U.S. Port.....	4
B. Security Boarding Procedures.....	7
1. Purpose.....	7
2. Authority	7
3. Discussion	8
4. Procedures.....	8
C. Security Compliance Examination Procedures: <i>ISPS/MTSA Security Compliance Examination and Non-Convention Vessel Security Compliance Examination</i>	11
1. Purpose.....	11
2. Applicability	11
3. Definitions.....	12
4. General.....	12
5. <i>ISPS/MTSA Security Compliance Examination Procedures at Sea</i>	13
6. <i>ISPS/MTSA Security Compliance Examination in Port</i>	21
7. <i>Non-Convention Vessel Security Compliance Examination</i>	28
D. Safety Compliance Examination Procedures: <i>Port State Control (PSC) Safety and Environmental Protection Compliance Examination</i>	35
1. Purpose.....	35
2. Authority	35
3. Procedures.....	35

Enclosure 4—Port Enforcement and Control Procedures

A. Enforcement.....	3
1. Philosophy.....	3
2. Provisions.....	3
Table 4-1: Vessel Types and Regulating Provisions and Authorities.....	7
B. Clear Grounds	8
Figure 4-1: Thresholds for clear grounds and control actions with security versus safety deficiencies.....	8
C. Vessel Control Procedures for Security and Safety	9
1. Denial of Entry/Expulsion	9
2. IMO Reportable Detentions.....	9

3.	Captain of the Port (COTP) Order	10
4.	Customs Hold	10
5.	Restriction of Operations/Vessel Movement	10
6.	Delay	11
7.	Comprehensive Security Inspection	11
8.	Letter of Deviation	11
9.	Flag State Notification	11
10.	Lesser Administrative/Corrective Measures	12
D.	Administrative Enforcement Measures (Apply to both security and safety violations)	12
1.	Civil Penalty Adjudication.....	12
2.	Civil Penalty.....	12
3.	Letter of Warning.....	12
4.	LOU / Surety Bond	13
E.	Port Enforcement and Control Measures	13
1.	Security Zone	13
2.	Naval Vessel Protection Zone (NVPZ) and Naval Protection Order	13
3.	Regulated Navigation Area (RNA).....	13
4.	Safety Zone	15
5.	Special Local Regulation (SLR)	15

Appendix A to Enclosure 4—Examples of Detainable Deficiencies for Security and Safety	A-2
---	-----

Enclosure 5—Glossary

Enclosure 6—Foreign Vessel Exam Book for MTSA/ISPS Code Compliance

ENCLOSURE 1

RISK-BASED TARGETING FOR ALL VESSELS

RISK-BASED TARGETING FOR ALL VESSELS

This enclosure details the guidelines and procedures for targeting vessels for boardings.

ENCLOSURE 1 - **Introduction**

A. Action – Using the Matrices

1. Targeting Philosophy – Security Compliance
2. Targeting Philosophy – Safety and Environmental Protection Compliance

Figure 1-1: Boarding Decision-Making Process for Each Vessel Arrival

B. Compliance Targeting Instructions (Step I & Step II)

1. Step I: *ISPS/MTSA Security Compliance Targeting Matrix*
2. Step II: *PSC Safety and Environmental Protection Compliance Targeting Matrix*
3. *Compliance Verification Examination Matrices*

C. Boarding Decision and Location (Step III)

1. ISPS I and Priority I (PI) Boardings
2. ISPS II and Priority II (PII) Boardings

D. Targeting Factor Criteria

1. Security Compliance Targeting Criteria
2. Safety and Environmental Protection Compliance Targeting Criteria

Table 1-1: Detention Ratios and Point Assignments

Introduction

To effectively implement the maritime security policy issued under the Maritime Transportation Security Act of 2002 (MTSA), and the International Ship and Port Facility Security (ISPS) Code, compliance actions will be seamlessly integrated into the existing port State control (PSC) program. The U.S. will be enforcing an expanded and comprehensive PSC program in order to identify and eliminate foreign merchant ships not in compliance with international Conventions and domestic rules from U.S. waters.

All vessels greater than 300 gross tons (GT) [soon to be 100 GT] are required to give a Notice of Arrival (NOA) to the National Vessel Movement Center (NVMC) prior to entering the United States (U.S.). These vessels will be screened, using three risk-based tools. These tools use a process known as Risk-Based Decision Making (RBDM) to determine the threat a vessel poses to a U.S. port. These RBDM tools, collectively referred to as the *Compliance Verification Examination Matrices*, will prioritize vessel boardings.

The first *Compliance Verification Examination Matrix* is a classified, risk-based tool used to evaluate the security risk of a vessel entering into port. (This risk analysis is not discussed in detail in this instruction because it is classified.) The second screening tool is used to evaluate a foreign-flag vessel's compliance with security standards. This screening is called the *ISPS/MTSA Security Compliance Targeting Matrix*. Because this matrix evaluates compliance to security standards, not security of the vessel itself, this screening is not classified. (Policy for U.S. vessel compliance with domestic security regulations is issued under different guidance.) The third risk-based screening evaluates a vessel's compliance with safety and environmental standards. This analysis is called the *Port State Control (PSC) Safety and Environmental Protection Compliance Matrix*. Like the other compliance matrix, it is also not classified. This screening tool was previously referred to as the *Foreign Vessel Targeting Matrix*.

Use of both the *ISPS/MTSA Security Compliance Targeting Matrix* and the *PSC Safety and Environmental Protection Compliance Targeting Matrix* allows for Captains of the Port (COTPs) to identify those vessels posing the greatest risk in all areas. When applied consistently, the targeting regime will ensure that vessels that pose the highest risk for noncompliance in all areas are boarded during every U.S. port call while vessels that pose lower risk of noncompliance are boarded less frequently.

A. Action – Using the matrices

All foreign-flag vessels required to submit an NOA to the NVMC should be screened using the *ISPS/MTSA Security Compliance Targeting Matrix*, for security compliance, and the *PSC Safety and Environmental Protection Compliance Targeting Matrix* (previously referred to as the *Foreign Vessel Targeting Matrix*), for safety and environmental compliance. These screening activities are required to identify those vessels that pose the greatest risk of noncompliance.

In addition, all vessels will be screened for the security risk they pose to U.S. ports. Vessels selected in this process are called high interest vessels (HIVs). While all vessels may be boarded on a random security boarding, these vessels are of higher interest to law enforcement

authorities. This enclosure will not provide details on this screening process, since it is discussed in a separate, classified instruction. Figure 1 provides a pictorial view of the three screening processes related to vessel examinations and security boardings that are applied to arriving vessels.

1. **Targeting Philosophy – Security Compliance**

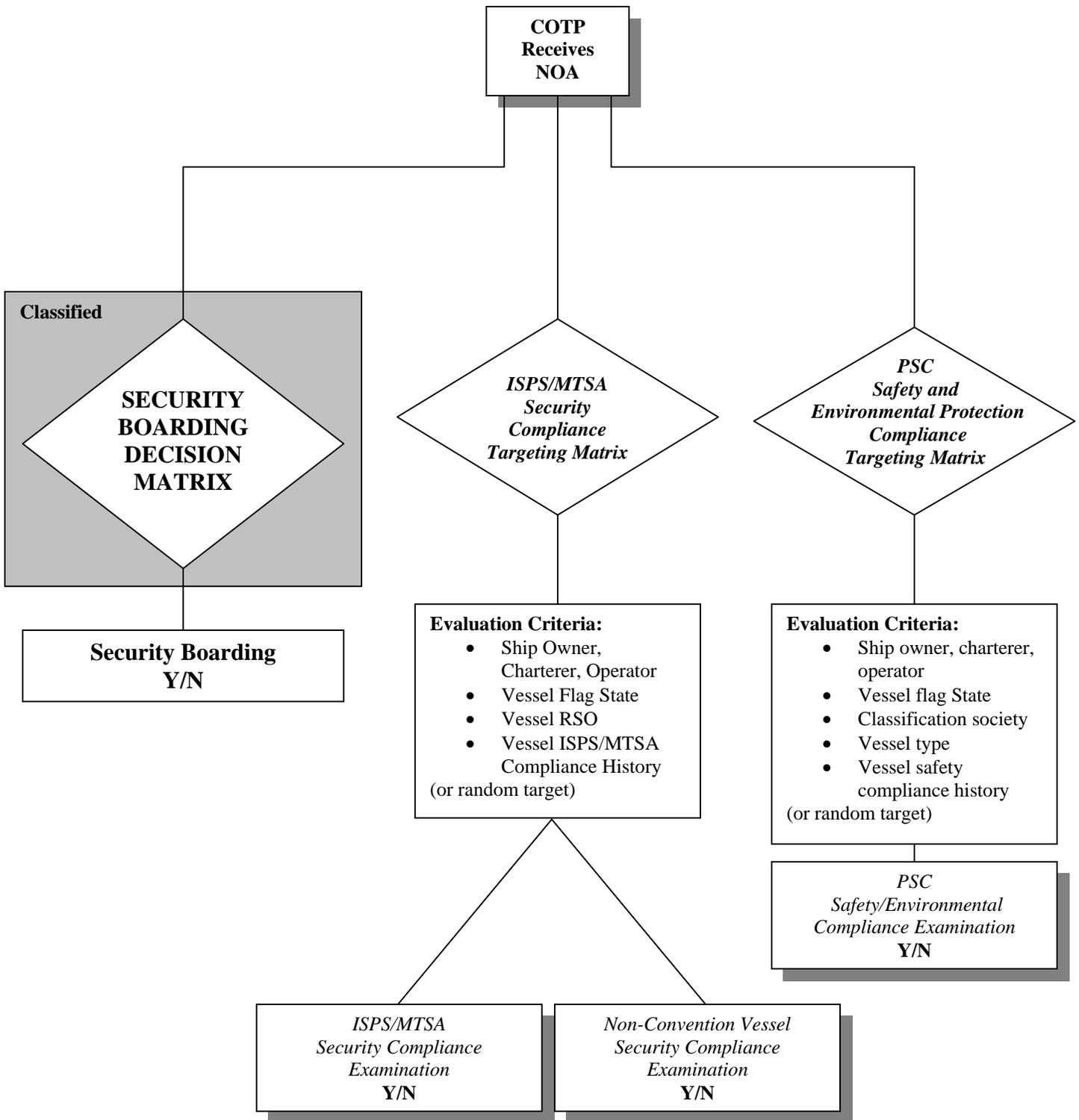
- a. **Applicable Factors.** The *ISPS/MTSA Security Compliance Targeting Matrix* is a screening tool that systematically evaluates several factors believed to contribute to a vessel's compliance or noncompliance with domestic and international maritime security standards. The *ISPS/MTSA Security Compliance Targeting Matrix* enables the USCG to systematically identify and target large commercial vessels (greater than 100 GT) that pose the greatest risk of noncompliance taking into consideration the following four risk factors: *ship management; flag State; recognized security organization (RSO)*, and the *individual vessel's security regulation compliance history* (the degree that vessel meets both domestic and international maritime security standards).
- b. **Functionality.** Using the *ISPS/MTSA Security Compliance Targeting Matrix*, points are assigned to a vessel based on the various risk factors. Assignment of points does not signify that the vessel is substandard; assignment of points only signifies that an examination should take place to determine the compliance of the vessel with domestic and international standards. The total points are compared to the point value thresholds to determine whether or not an examination should take place. Total points also determine where an examination should take place.
- c. **Consistency.** To be effective, it is important that this targeting regime be applied consistently. In addition to focusing USCG resources, the *ISPS/MTSA Security Compliance Targeting Matrix* serves to consistently place the onus for maintaining vessels to accepted standards on those most responsible including ship management, RSOs, and flag States. Linking boarding decisions to the performance records of the ship, the ship's management, the RSO, and the flag State helps ensure consistent accountability.
- d. **Random Vessel Targeting:** During the initial period of enforcement, every vessel visiting the U.S. will be examined at least once. After this initial period, the *ISPS/MTSA Security Compliance Targeting Matrix* will identify those vessels posing the greatest risk of noncompliance with SOLAS Chapter XI-2, the ISPS Code, and the regulations issued under MTSA. In addition, the COTP will randomly examine a certain percentage of the vessels that do not screen for a security compliance examination. Such random examinations should normally be conducted in port, but may be combined with other examinations scheduled for the vessel as it arrives.

2. **Targeting Philosophy- Safety and Environmental Protection Compliance**

- a. **Applicable Factors.** A targeting regime has been successfully used to consistently

- focus Coast Guard port State control efforts since 1994. This risk-based approach evaluates vessels using five factors. These factors are a *ship management, flag State, classification society, compliance history* and *vessel type*. The risks associated with each of these factors are evaluated using Coast Guard boarding data developed over previous years. Points are assigned based on performance and using the targeting matrix, which subsequently determines a safety boarding priority.
- b. Functionality. Using the *PSC Safety and Environmental Protection Compliance Targeting Matrix*, points are assigned to a vessel based on the various risk factors. Assignment of points does not signify that the vessel is substandard; assignment of points only signifies that a boarding and examination should take place to determine the compliance of the vessel with international standards.
 - c. Consistency. To be effective, it is important that this targeting regime be applied consistently. In addition to focusing USCG resources, the *PSC Safety and Environmental Protection Compliance Targeting Matrix* serves to place the onus for maintaining vessels to accepted standards on those most responsible including ship management, classification societies and flag States. Linking boarding decisions to the performance records of the ship, the ship's management, classification society and flag State helps ensure accountability.
 - d. Random Vessel Targeting: The *PSC Safety and Environmental Protection Compliance Targeting Matrix* will identify those vessels posing the greatest risk of noncompliance with safety and environmental protection aspects of SOLAS. In addition, the COTP will randomly examine a certain percentage of the vessels that do not screen for an examination. Such random examinations should normally be conducted in port, but may be combined with other examinations scheduled for the vessel as it arrives.

Figure 1-1: Boarding Decision-Making Process for Each Vessel Arrival



B. Compliance Targeting Matrix Instructions (Step I & Step II)

1. Step I: ISPS/MTSA Security Compliance Targeting Matrix

As stated previously, the *ISPS/MTSA Security Compliance Targeting Matrix* is a tool for the COTP to determine whether a particular vessel scheduled to arrive should be targeted for examination. NOA information and Marine Information for Safety and Law Enforcement (MISLE) data shall be used to determine a score. This needs to be done manually until an automated, MISLE-embedded targeting tool is completed. The score calculated for a particular vessel will determine whether a vessel is examined at sea, examined in port, or not targeted (all vessels are subject to random selection).

Criteria to make security examination decisions are based on the *control action ratio* (CAR). The CAR is similar to the *detention ratio* that is used to make PSC safety/environmental protection examination decisions. The CAR scoring index will be calculated and provided by the Foreign and Offshore Compliance Division (G-MOC-2). The CAR is defined below and calculated based on the previous three years. CAR data accumulation begins on 1 July 2004. *# of major ISPS/MTSA-related control actions* include security-related denials of entry or expulsions from port, as well as security-related detentions, within the period of interest.

$$\text{CAR} = \frac{\text{\# of major ISPS/MTSA-related control actions}}{\text{\# of ISPS/MTSA examinations}} \times 100 \text{ percent}$$

- a. Column I: Ship Management For the purposes of ship management targeting for ISPS compliance, the CAR is defined below. *# of major ISPS/MTSA-related control actions* include security-related denials of entry or expulsions from port, as well as security-related detentions, within the period of interest.

$$\text{CAR} = \frac{\text{\# of major ISPS/MTSA-related control actions}}{\text{\# of ISPS/MTSA examinations}} \times 100 \text{ percent}$$

- 1) If MISLE data indicates that the owner, operator, or charterer has been associated with any vessel that has been the subject of ISPS security control actions involving denial of entry or expulsion from port within the last 12 months, *assign ISPS I status to the vessel*. (See section 3, Compliance Targeting Matrices, for further information of *ISPS status*.) The COTP may relax status to ISPS II depending on the circumstances of the control action (example: If the Security Plan was not properly implemented, and the owner has since initiated steps to correct security implementation.) Assign 2 points if entry was denied due solely to lack of proper NOA.
- 2) If the owner, charterer, or managing operator of a vessel is included on the Targeted Ship Management List provided by the Office of Compliance (G-MOC),

assign 5 points.

- 3) If the owner, charterer, or managing operator is associated with more than 10 vessel examinations in the last three years, beginning July 1, 2004, and has a CAR greater than 5 percent during that period, assign 5 points.
 - 4) If the owner, charterer, or managing operator of a vessel is associated with more than 10 vessel examinations in the past three years, beginning 1 July 2004, and has a CAR greater than 1 percent, but up to 5 percent during that period, assign 2 points.
 - 5) If the owner, charterer or managing operator of a vessel has been associated with 10 or fewer vessel examinations in the past three years, beginning 1 July 2004, assign 2 points.
 - 6) A maximum total of 5 points may be assigned.
 - 7) Proceed to Column II.
- b. Column II: flag State The CAR is defined below for the purposes of flag State targeting for compliance. *# of major ISPS-related control actions* include all security-related denials of entry or expulsions from port and ISPS-related detentions to vessels flying the flag of that State within the period of interest.

$$\text{CAR} = \frac{\text{\# of major ISPS/MTSA-related control actions}}{\text{\# of ISPS/MTSA examinations}} \times 100 \text{ percent}$$

- 1) Check the vessel's flag State against the current targeted flag State list. If the flag State is listed as a targeted flag State, assign 7 points. Listing criteria: Flag State is associated with more than 20 vessel examinations in the past three years, beginning 1 July 2004, and has a CAR greater than 5 percent during that period.
 - 2) If the flag State of a vessel is associated with more than 20 vessel examinations in the past three years, beginning 1 July 2004, and has a CAR greater than 1 percent, but up to 5 percent during that period, assign 2 points.
 - 3) If the flag Administration of a vessel has been associated with 20 or fewer vessel examinations in the past three years, beginning 1 July 2004, assign 2 points.
 - 4) Proceed to Column III.
- c. Column III: Recognized Security Organization (RSO) For the purposes of RSO targeting for ISPS compliance, the CAR is defined below. *# of major ISPS-related control actions* include security-related denials of entry or expulsions from port and ISPS-related detentions *attributable to the RSO* within the period of interest. Control actions are attributable to the RSO when a procedure in the RSO-approved security

plan does not conform to SOLAS Chapter XI-2 and the ISPS Code or when a security procedure verified by the RSO does not conform to the approved security plan. When the flag State does not allow an RSO to act on its behalf, Column III may also be used to add points for targeting the flag State when the ISPS/MTSA control actions discussed herein are attributable to the flag State (in similar fashion to that for an RSO).

$$\text{CAR} = \frac{\text{\# of major ISPS/MTSA-related control actions}}{\text{\# of ISPS/MTSA examinations}} \times 100 \text{ percent}$$

- 1) Check the vessel's RSO against the current targeted RSO list. Listing criteria: If the RSO is associated with more than 20 vessel examinations in the past three years, beginning 1 July 2004 and has a CAR greater than 5 percent during that period, assign ISPS I status to the vessel.
 - 2) If the RSO is associated with more than 20 vessel examinations in the past three years, beginning 1 July 2004 and has a CAR greater than 1 percent and up to 5 percent, assign 5 points; or has a CAR greater than 0.5 percent and up to 1 percent, assign 2 points.
 - 3) If the RSO of a vessel has been associated with twenty or fewer vessel examinations in the past three years, beginning 1 July 2004, assign 2 points.
 - 4) Proceed to Column IV.
- d. Column IV: Vessel ISPS/MTSA Compliance History
- 1) If MISLE data indicates that the vessel has been the subject of ISPS security control actions involving denial of entry or expulsion from port within the past 12 months, assign ISPS I status to the vessel.
 - a. The COTP may relax status to ISPS II depending on circumstances of control action (Example: The vessel was expelled from port because of failure to implement security plan procedures, but has corrected the situation and compliance was verified by USCG subsequent examination.)
 - b. If denial of entry due solely to lack of proper NOA, assign 2 points.
 - c. G-MOC will enter an inspection note after reviewing detention reports received from field units. This notice will assist in identifying vessels detained within the previous 12 months, *but may not include very recent detentions*. Field units must check the MISLE Vessel Critical Profile to determine whether any recent detentions have occurred.
 - 2) If MISLE data indicates the vessel has not been examined for compliance with

SOLAS Chapter XI-2 and the ISPS Code in the past 12 months, assign ISPS II status to the vessel.

- 3) If MISLE data indicates that the vessel has CAR greater than 1 percent, assign 5 points to the vessel.
- 4) If MISLE data indicates that the vessel has CAR greater than 0.5 percent and up to 1 percent, assign 2 points to the vessel.
- 5) If MISLE data indicates that the vessel has been examined more than once, but ten or fewer times in the past 3 years, for compliance with SOLAS Chapter XI-2 and the ISPS Code, assign 2 points.
- 6) If MISLE data indicates that the vessel has had any ISPS or MTSA-related operational control, excluding denial of entry, expulsion from port, or detentions, assigned within the last 12 months, assign 1 point for each operational control.
- 7) The total points in Column IV are unlimited.
- 8) Proceed to Total.

e. Total

Total the assigned points from each column. Note the *ISPS status* below:

17 or more points = **ISPS I Vessel**

7 to 16 points = **ISPS II Vessel**

0-6 points = **ISPS III Vessel**

2. Step II: PSC Safety and Environmental Protection Compliance Targeting Matrix

This matrix is automatically calculated in MISLE once the vessel has been imported from the Ship Arrival Notification System (SANS); however, the Boarding Wizard must be used to complete the final score. For details regarding these tools, refer to the MISLE user guide at http://mislenet.osc.uscg.mil/user_guides.aspx

a. Column I: Ship Management

- 1) If the owner, charterer or managing operator of a vessel is included on the current Targeted Owners List provided by G-MOC, assign 5 points.
- 2) A maximum total of 5 points may be assigned.
- 3) Proceed to Column II.

b. Column II: Flag

1) Check the vessel's flag State against the current targeted flag State list. If the flag State is listed as a targeted flag State, assign 7 points.

2) Proceed to Column III.

c. Column III: Classification Society

1) Check the vessel's classification society against the current targeted classification society list. If the classification society is listed as a targeted classification society, assign the appropriate number of points as indicated at <http://cgweb.comdt.uscg.mil/g-mo/moc/mochm.htm>.

2) Proceed to Column IV.

d. Column IV: Vessel History

1) If MISLE data indicates that the vessel has been the subject of an intervention leading to detention within the past 12 months, assign 5 points for each detention. An inspection note is entered by G-MOC after reviewing detention reports received from field units. This notice will assist in identifying vessels detained within the previous 12 months, but may not include very recent detentions. Field units must check the MISLE Vessel Critical Profile to determine whether any recent detentions have occurred.

2) If MISLE data indicates that the vessel has been the subject of any other form of operational control within the past 12 months (i.e., COTP Order or Customs hold), assign 1 point for each incident. Do not assign multiple points where more than one control action was taken for a single incident.

3) If MISLE data indicates that the vessel has been involved in any marine casualty or pollution cases within the past 12 months, assign 1 point for each case.

4) If MISLE data indicates that the vessel has been the subject of a marine violation, except for pollution, within the past 12 months, assign 1 point for each violation case.

5) If MISLE data indicates the vessel has not been boarded in the past 6 months, assign a maximum of 1 point for this category.

6) The total points in Column IV are unlimited.

7) Proceed to Column V.

e. Total

(1) Total the assigned points from each column. Note the priority status below:

17 or more points = **Priority I Vessel (PI)**

7 to 16 points = **Priority II Vessel (PII)**

0-6 points = **Non Priority Vessel (NPV)**

3. Compliance Verification Examination Matrices

STEP I: ISPS/MTSA Security Compliance Targeting Matrix

COLUMN I	COLUMN II	COLUMN III	COLUMN IV
SHIP MANAGEMENT	FLAG STATE	RECOGNIZED SECURITY ORGANIZATION	SECURITY COMPLIANCE HISTORY
<p>ISPS I</p> <p>Owner, operator, charterer associated w/ ISPS-related denial of entry/expulsion from port in past 12 months *</p> <p>5 Points</p> <p>Owner, Operator, or Charterer has a CAR of 5 percent or more or is on the G-MOC Targeted Ship Management List</p> <p>2 Points</p> <p>Owner, Operator, or Charterer has a CAR of 1 percent, and up to 5 percent</p> <p>2 Points</p> <p><i>Owner, Operator, or Charterer associated w/ 10 or fewer vessel examinations in the past 3 years beginning 1 July 2004</i></p>	<p>7 Points</p> <p>Flag State has a CAR of 5 percent or more</p> <p>2 Points</p> <p>Flag State has a CAR from 1 percent to 5 percent</p> <p>2 Points</p> <p><i>Flag State associated w/ 20 or fewer vessel examinations in the past 3 years beginning 1 July 2004</i></p>	<p>ISPS I</p> <p>RSO has a CAR of 5 percent or more</p> <p>5 Points</p> <p>RSO has a CAR of 1 percent, and up to 5 percent</p> <p>2 Points</p> <p>RSO has a CAR of 0.5 percent, and up to 1 percent</p> <p>2 Points</p> <p><i>RSO associated w/ 20 or fewer vessel examinations in the past 3 years beginning 1 July 2004</i></p> <p>Note: Use RSO attribution process for flag States not using RSOs</p>	<p>ISPS I</p> <p>ISPS-related denial of entry/expulsion from port in past 12 months *</p> <p>ISPS II</p> <p><i>No ISPS compliance examination within the past 12 months</i></p> <p>5 Points</p> <p>Vessel has a CAR of 1 percent or more</p> <p>2 Points</p> <p>Vessel has a CAR of 0.5 percent, and up to 1 percent</p> <p>2 Points</p> <p><i>More than one, but 10 or fewer ISPS Compliance examinations in the past 3 years beginning 1 July 2004</i></p> <p>1 Point</p> <p>For each occurrence of any operational control assigned w/ past 12 months</p>

Italics indicate applicable scoring criteria at the onset of MTSA/ISPS enforcement. Non-italicized criteria will require time to develop sufficient owner, operator, charterer, Flag, RSO, and vessel history

* Depending upon circumstances of denial of entry, COTP may relax assignment to ISPS II. Also, if denial of entry due solely to failure to provide NOA, assign 2 points

Vessels that score 17 points or higher are ISPS I vessels and must be boarded prior to port-entry.

Vessels that score between 7-16 points are ISPS II vessels and need not be examined prior to entry but should be examined upon port arrival.

Vessels scoring fewer than 7 points are ISPS III vessels and need not be boarded unless selected at random for random MTSA/ISPS examination.

STEP II: PSC Safety and Environmental Protection Compliance Targeting Matrix

COLUMN I	COLUMN II	COLUMN III	COLUMN IV	COLUMN V
SHIP MANAGEMENT	FLAG STATE	CLASSIFICATION SOCIETY	VESSEL HISTORY	SHIP TYPE
5 Points Listed Owner, Operator, or Charterer	7 Points Listed Flag State	Priority 1 A detention ratio equal to or greater than 2%	5 Points Each Detention within the previous 12 months.	1 Point Oil or Chemical Tanker
		5 Points A detention ratio equal to 1% or less than 2%	1 Point Each Other operational control within the previous 12 months	1 Point Gas Carrier
		3 Points A detention ratio equal to 0.5% or less than 1%	1 Point Each Casualty within the previous 12 months.	2 Points Bulk Freighter over 10 years old.
		0 Points A detention ratio less than 0.5%	1 Point Each Violation within the previous 12 months.	1 Point Passenger Ship
			1 Point Each Not boarded within the previous 6 months.	2 Points Carrying low value commodities in bulk.

Vessels that score 17 points or higher are Priority I vessels and must be boarded prior to port-entry.

Vessels that score between 7-16 points are Priority II and need not be examined prior to entry but should be examined upon port arrival.

Vessels scoring fewer than 7 points are Non Priority Vessels (NPV). These vessels are also known as Priority III and Priority IV vessels and need not be boarded. No operational restrictions are imposed on Priority III and Priority IV vessels.

C. Boarding Decision and Location (Step III)

The *ISPS/MTSA Security Compliance Targeting Matrix* and *PSC Safety and Environmental Protection Compliance Targeting Matrix* evaluate a vessel's relative risk of noncompliance with maritime security and safety standards and results in the assignment of points. Each matrix will provide a total that corresponds to the designations of ISPS I/ISPS II/ISPS III and PI/PII/PIII. Once this evaluation has been done, the COTP must decide on the location and timing of the boarding as well as appropriate risk mitigation measures.

ISPS I and PI boardings require a significant commitment of resources and time as they require boarding personnel with significant skill sets and they, in most cases, will occur at the sea buoy. They may also result in some type of risk mitigation measure during the inbound

transit such as vessel escort or armed personnel onboard. COTP's must prioritize how boarding resources are deployed to ensure that those vessels representing the highest risk to the port from both a security and safety aspect are boarded.

1. ISPS I Vessels and Priority I (PI) Vessels. ISPS I and PI vessels shall be boarded prior to port entry. Exceptions to the at-sea boarding requirement for ISPS I and PI vessels may be made by the COTP. (The COTP may make an exception if the boarding presents a risk to personnel or the logistics of an at-sea boarding are impractical.) The at-sea boarding location shall be designated by the COTP. The COTP should consider local geography, the safety and security of the port, space for maneuvering, and safety of personnel during at-sea transfers when designating the at-sea boarding area.
2. ISPS II and Priority II (PII) Boardings. While ISPS II and PII designated vessels theoretically represent a smaller risk, they still require assignment of significant boarding resources. PII exams will normally be conducted pier-side prior to the loading or offloading of cargo and passengers. ISPS II examinations should begin before loading or offloading commence, but may continue during loading/offloading operations so that security procedures related to cargo and passenger embarkation operations may be observed. COTPs ultimately have to make a determination of what the most appropriate boarding procedure should be for each individual case.

D. Targeting Factor Criteria

To implement the targeted compliance examination regime, it is necessary to identify which vessels, vessel owners, flag Administrations and RSOs are most often associated with substandard ships. These determinations are made by G-MOC based on Coast Guard boarding and intervention data and will be promulgated regularly by monthly message.

1. Security Compliance Targeting Criteria (effective 1 July 2004)

This section provides a more detailed explanation regarding the security risk factors listed in the *ISPS/MTSA Security Compliance Targeting Matrix*. Criteria to make security examination decisions have been established. A common element integral to many of the criteria is the CAR, which is similar to the detention ratio used to make PSC safety compliance examination decisions. The CAR is generally defined below. The # of major *ISPS-related control actions* include security-related denial of entry or expulsion from port (within the 12 to 36 month period prior to the current vessel arrival). It also includes security-related detentions within the last three years, beginning on 1 July 2004. The # of *ISPS examinations* include a specified minimum number of distinct ISPS examinations.

$$\text{CAR} = \frac{\text{\# of major ISPS-related control actions}}{\text{\# of ISPS examinations}} \times 100 \text{ percent}$$

Where the targeting matrix refers to an "at-sea" boarding, the location should be designated by the COTP based upon considerations including local geography, the safety and security of the port, sufficient sea room for maneuvering, and safety of personnel during at-sea transfers

of personnel from the boarding platform to the vessel.

a. Targeted Ship Management - Targeted ship management includes any owner, operator, charterer or managing operator who is associated with a vessel that has been denied port entry, been expelled from port, or detained within a specified range of time and has been assigned a CAR based on MISLE control action information.

- (1) Targeted Ship Management List. G-MOC will develop and maintain a monthly listing of targeted owners based on CARs received from field units.
- (2) Application. All vessels associated with owner, operator, or charterer having a CAR of 1 percent or more will receive points towards the security examination decision. With certain exceptions as noted in the *ISPS/MTSA Security Compliance Targeting Matrix*, vessels linked to an owner, operator, or charterer associated with an ISPS/MTSA-related denial of entry or expulsion from port will be targeted for an at-sea security compliance examination.
- (3) Downgrading and Removal. As performance improves, a targeted ship manager will receive fewer points or be removed from the list. The targeted ship manager will be removed from the list if the CAR associated with that entity drops below 1.0 percent.

b. Targeted Flag Administration - A targeted flag Administration includes any flag State that is associated with a vessel that has been denied port entry, been expelled from port, or detained within a specified range of time and has been assigned a CAR based upon MISLE control action information.

- (1) Flag Administration CAR for Security Compliance. G-MOC will develop and maintain a monthly listing of targeted owners based on CARs received from field units.
- (2) Application. All vessels associated with a flag Administration having a CAR of 1 percent or more will receive points towards the security compliance examination decision.
- (3) Removal. As performance improves, a targeted flag Administration will receive fewer points or be removed from the list. The targeted flag Administration will be removed from the list if the CAR associated with that entity drops below 1.0 percent.
- (4) Release of Information. The targeted flag Administration list for security compliance performance will be published in the PSC Annual Report as well as on the PSC website at <http://www.uscg.mil/hq/g-m/pscweb/flag.htm>.

c. Targeted Recognized Security Organization (RSO)

- (1) Recognized Security Organization. An RSO is the organization with the appropriate expertise in security and anti-terrorism matters recognized by the Administration (or Designated Authority) and authorized to carry out assessment, verification, approval and certification activities, required by the ISPS Code.
- (2) Targeted RSO. G-MOC will develop and maintain a monthly listing of targeted RSOs based on control action reports received from field units.
- (3) Application. All vessels associated with an RSO having a CAR of 1 percent or to 5 percent will receive points towards the security compliance examination decision. Any vessel associated with an RSO having a CAR more than 5 percent will be targeted for an at-sea security compliance examination.
- (4) Removal. As performance improves, a targeted RSO will receive fewer points or be removed from the list. The targeted flag Administration will be removed from the list if the CAR associated with that entity drops below 1.0 percent.
- (5) Release of Information. The targeted RSO list for security compliance performance will be published in the PSC Annual Report as well as on the PSC website at <http://www.uscg.mil/hq/g-m/pscweb/flag.htm>.

2. Safety and Environmental Protection Compliance Targeting Criteria

To implement the targeted boarding regime, it is necessary to identify which vessels, vessel management, classification societies, and flag States are most often associated with substandard ships. These determinations are made by G-MOC based on Coast Guard boarding and intervention data. To understand how these determinations are made, it is necessary to define certain terms of reference.

a. Targeted Ship Management

A targeted ship management includes any owner, operator, charterer, or managing operator whose vessels have been detained in the U.S. more than once within the previous 12 months under the provisions of an international Convention. If a vessel owner, operator or charterer has at least 25 vessels that visit U.S. ports each year, the company will not be targeted unless it accumulates 3 or more detentions within a 12-month period.

- (1) Targeted Ship Management List. G-MOC develops and maintains a current listing of targeted ship managers based on detention reports received from field units. The list is updated monthly.
- (2) Application. All vessels associated with a targeted owner receive 5 points under Column I of the *PSC Safety and Environmental Protection Compliance Targeting Matrix*.

- (3) Removal. A targeted owner is removed from the list if they are associated with less than two detentions carried out under the authority of an international convention within the previous 12 months.

b. Targeted Flag Administration

A targeted flag Administration is a country with a safety-related detention ratio exceeding the average safety detention ratio for all flag Administrations with vessels operating in U.S. waters.

- (1) Flag Administration Safety Detention Ratio. A flag Administration's safety detention ratio is calculated by dividing the number of its vessels detained under the authority of an international convention by the number of vessels under its registry, which entered U.S. waters. An average safety detention ratio for all flag Administrations with vessels operating in U.S. waters is obtained by dividing the number of vessels detained under the authority of an international convention by the number of vessels that entered U.S. waters. Individual flag Administration detention ratios are calculated based on the previous three years' data to reduce the effects of any anomalies.
- (2) Targeted Flag Administration List. This list consists of the targeted flag Administrations compiled by G-MOC on an annual basis for use with the *PSC Safety and Environmental Protection Compliance Targeting Matrix*. The list can be found on the Web at <http://www.uscg.mil/hq/g-m/pscweb/flag.htm>
- (3) Application. All vessels registered with a targeted flag Administration are assigned 7 points in Column II of the *PSC Safety and Environmental Protection Compliance Targeting Matrix*.
- (4) Removal. A targeted flag Administration is removed from the list when its safety detention ratio drops below the average safety detention ratio for all flag Administrations with vessels operating in U.S. waters or when it is associated with less than two detentions carried out under the authority of an international Convention within the past 12 months.

c. Targeted Classification Society

Classification Societies are evaluated on their performance over the previous three years to normalize the data. If they have a 3-year safety detention ratio that exceeds the fixed 3-year safety detention ratio (0.5%), then they will receive points. See the Classification Society chart below for details.

- (1) Classification Society. A classification society is an organization, other than a flag State that issues Certificates of Class or International Convention Certificates. When working on behalf of a flag Administration they are

referred to as Recognized Organizations (ROs).

- (2) Targeted Classification Society List. The Targeted Classification Society List contains the names of classification societies that will receive points in the *PSC Safety and Environmental Protection Compliance Targeting Matrix*.
- (3) Classification Society Detention Ratios. Classification society performance is based on their class-related safety detention ratio (number of class-related safety detentions divided by the number of distinct arrivals over a 3-year period). This ratio is then compared to the fixed ratios of acceptable performance. These classification societies are then assigned points according to where their safety detention ratios fall. See Table 1-1 below:

Table 1-1: Detention Ratios and Point Assignments

Classification Society's 3-year Detention Ratio	Matrix Point Assignment
A detention ratio less than 0.5%	0 Points
A detention ratio equal to 0.5% or less than 1%	3 Points
A detention ratio equal to 1% or less than 2%	5 Points
A detention ratio equal to or greater than 2%	Priority I

ENCLOSURE 2

REPORTING AND NOTIFICATION PROCEDURES

REPORTING AND NOTIFICATION PROCEDURES

This enclosure details reporting and notification requirements for port State control detentions and for related maritime homeland security issues.

ENCLOSURE 2: **Introduction**

A. Security and Safety-Related Detentions, Unit Responsibilities

1. Flag State Notification
2. USCG Headquarters/Area/District Notification
3. Classification Society/Recognized Organization/Recognized Security Organization Notification
4. Ship Management Notification

B. Security and Safety-Related Detentions, USCG Headquarters Responsibilities

1. Owner Notification
2. International Maritime Organization Notification

C. IMO Detention Notification Responsibility Chart

D. Documentation

1. Detentions
2. Deficiency Compliance Dates
3. Deficiency Format

Introduction

Notification and reporting procedures have been streamlined into a single reporting process consolidating information related to Ports, Waterway, and Coastal Security (PWCS) and port State control (PSC). To the greatest extent possible, reports must be consolidated to fulfill the needs of all stakeholders. The report is intended to support various functions including administrative recordkeeping, resource alignment, statistical purposes, congressional mandates, and program management. This single report is also designed to meet our reporting obligations to the International Maritime Organization (IMO).

This single report of PSC activity consists of Form A and Form B, which have been designed in accordance with the IMO Procedures for Port State Control Resolution A.787(19), as amended by A.882(21). It is imperative that units use the stock system forms without modification. These forms are updated periodically to coincide with the latest IMO guidance and Coast Guard policy.

These procedures will replace all existing notification requirements, and are intended to simplify efforts at the Captain of the Port (COTP) level. The basic premise behind the new reporting procedures involves electronically scanning forms. The unit member should electronically “scan in” both Forms A and B, and then email these reports to the cognizant authorities. Senders should request a return receipt as documentation of chain of custody control. (To request a return receipt from a Microsoft Outlook message, click “File” then “Properties.” Next, check the box next to the appropriate “receipt requested” box.) For a historical reference, these scanned forms should also be attached in the Marine Information for Safety and Law Enforcement (MISLE) system under the respective vessel in the documentation section. It is crucial that legible handwriting is used and correct cites are researched and entered on these forms.

A. Security and Safety-Related Detentions, Unit Responsibilities

Whenever a foreign vessel has an intervention leading to detention, several notifications must be conducted by the COTP regardless of whether the detention is due to a security-related or safety-related issue. Unit responsibilities are summarized in the table entitled, “IMO Detention Notification Responsibility Chart,” located in section C of this enclosure.

1. Flag State Notification. Whenever a foreign vessel is denied entry to a port or offshore terminal, or is detained for a safety or security reason, the unit taking that action must notify the flag State as soon as possible. Points of contact are provided on the PSC website at <http://www.uscg.mil/hq/g-m/pscweb/index.htm>. IMO Assembly Resolution A.787(19), as amended by A.882(21), requires that port States initiating control actions notify the flag Administration forthwith. For maritime security-related control actions such as inspection of the ship, delaying the ship, detention of the ship, restriction of operations, including movement within the port, or expulsion of the ship from the port, the unit making the control action must also notify the flag State as soon as possible. Notification should be in writing within 24 hours of initiating the action. Submitting Forms A and B is an acceptable means of notifying the flag State. Should difficulties be

encountered in making this notification, contact the Commandant, Foreign and Offshore Compliance Division (G-MOC-2) for additional information at (202) 267-0495 or (202) 267-2978.

2. Headquarters/Area/District Notification. When deficiencies are found to be detainable under international instruments such as SOLAS, units are directed to scan and then email both the *USCG Port State Control Report of Inspection, Form A (CG-5437A)* and the *USCG Port State Control Report of Inspection, Form B (CG-5437B)* to G-MOC-2 at fldr-g-moc@comdt.uscg.mil The forms must be completed as described below.
 - a. The forms are required to be submitted to G-MOC-2 when the vessel is detained (if form A, Block 17 is marked “Yes”). If units cannot email the forms, they should contact G-MOC-2 for alternate submission approval.
 - b. Both forms must be filled out completely and accurately. Any incomplete forms will be returned to the unit for resubmission.
 - c. All deficiencies identified and approved by the cognizant Officer in Charge of Marine Inspection (OCMI) or COTP as detainable under SOLAS, must be clearly annotated with a “D” and placed on Form B (CG-5437B), under the “Action Taken” category. The deficiency must clearly state the grounds for detention.
 - d. To ensure quality control for all detention reports, Form B must be signed by the port State control officer’s (PSCO’s) supervisor, a Marine Safety Detachment (MSD) Supervisor, or Chief of Inspections Department (CID). The supervisor’s signature and printed name must be placed on the lower right side of Form B.
 - e. Delivery of the report to the Office of Compliance (G-MOC) should be as soon as possible, but must be scanned and delivered to G-MOC no later than 1630 EST/EDT on the next business day following the detention.
3. Classification Society/Recognized Organization/Recognized Security Organization Notification. The local office of the classification societies, Recognized Organization (RO), or Recognized Security Organization (RSO) that issued the relevant certificates to a detained vessel must be notified of the detention. A visit by the local surveyor or class representative can expedite the deficiency correction process. The delivery of the completed report to the Classification Society, RO or RSO should be as soon as possible, but must be sent no later than 1630 on the next business day following the detention. A list of points of contact for class societies is provided on the port State control Website at <http://www.uscg.mil/hq/g-m/pscweb/index.htm>. Submission of Forms A and B is acceptable as a form of notification.
 - a. Involvement of RO and RSOs in the correction of deficiencies related to equipment, hull, structure or security items is strongly encouraged. To ensure accountability, the OCMI or COTP should advise G-MOC of unsatisfactory performance of these organizations rather than corresponding directly.

- b. Upon review, G-MOC will officially notify the organization of any detentions determined to be the result of deficiencies for which the organization should be held accountable. When a detention is attributed in this manner it is tracked and used to determine the annual performance for the organization. The annual performance for each organization is used to develop and publish the targeted lists for the boarding matrices.
4. Ship Management Notification. The command should ensure that the owner, operator, master, or charterer of the vessel is given a copy of the boarding reports (Forms CG-5437A and CG-5437B) and a clear work list of actions that must be taken to correct all deficiencies. Before the vessel will be permitted to leave port, any outstanding items listed on the forms must be addressed and should be clearly marked and explained.

B. Security and Safety-Related Detentions, USCG Headquarters Responsibilities

USCG Headquarters responsibilities are summarized in the table entitled, "IMO Detention Notification Responsibility Chart," located in section C of this enclosure.

1. Ship Management Notification. Upon receipt of the boarding reports (Forms CG-5437A and CG-5437B), G-MOC will send written notification to the owner, operator, managing operator, and charterer of the vessel. This is normally conducted within 45-60 days of the detention.
2. IMO Notification. When an intervention leads to a detention, G-MOC submits a report to IMO to fulfill the reporting procedures as required by various international instruments. This is normally conducted within 45-60 days of the detention.

C. IMO Detention Notification Responsibility Chart: Unit and USCG Headquarters responsibilities are summarized in the following table.

Table 2-1: IMO Detention Notification Responsibility Chart

	Complete Form A and B and scan documents. Attach scanned versions to activity in MISLE	Notify Master and give copy of Form A and B	Email or Fax Form A and B to Ship Management	Email or Fax Form A and B to Recognized Security Organization or Classification Society	Email or Fax Form A and B to Flag State	Email or Fax Form A and B to HQ by close of business next working day	Ship Management Notification Letter	IMO Notification Letter	Notify Port State Control Memorandums of Understanding / Agreements
Unit Notification Responsibility for Security-Related Detention	XX	XX	XX	XX	XX	XX			
Unit Notification Responsibility for Safety-Related Detention	XX	XX	XX	XX	XX	XX			
HQ Notification Responsibility for Security or Safety- Related Detention							XX	XX	
Unit Notification Responsibility for Ship Denied Entry for Safety or Security	XX	XX	XX	XX	XX	XX			
HQ Notification Responsibility for Ship Denied Entry for Safety or Security							XX	XX	XX

D. Documentation

1. Detentions: All vessels detained shall have corresponding MISLE activities entered into the system within 24 hours of the detention. The unit shall create an operational control and pick a MISLE Control Type of “PSC Safety Detention” or “PSC Security Detention” **only** for detentions that are to be reported to IMO. **If a different control type is chosen, it will not initiate the required Headquarters review of the detention case.** If a foreign vessel is subject to an operational control but has not violated an international instrument, then units must select another control type such as “COTP Order” or “U.S. Customs Clearance Hold”. For more information on using MISLE applications, you can access several MISLE user guides by visiting MISLENET on the Web: http://mislenet.osc.uscg.mil/user_guides.aspx.
 - a. Security-Related Detentions. Deficiencies should clearly state what problems exist and the scope or seriousness of the deficiencies. For example, “Vessel inadequately attained appropriate security level, as required by Declaration of Security (DoS) with port facility, due to lack of access control to the ship and unsuitable handling of unaccompanied baggage”, provides a more detailed description of the problem than to state “Violation of DoS”. Applicable cites shall be entered for all deficiencies listed on the Detention Report (CG-5437B).
 - b. Safety-Related Detentions. Deficiencies should clearly state what problems exist and the scope or seriousness of the deficiencies (for example "Firemain, multiple holes, 60% wastage - unable to maintain adequate pressure). Applicable cites shall be entered for all deficiencies listed on the Detention Report (CG-5437B).
2. Deficiencies Compliance Dates: Each deficiency shall be assigned a compliance date appropriate to the nature of the deficiency. The length of time allowed to correct the deficiencies is left to the discretion of the OCMI or COTP. In making the determination, the OCMI or COTP should consider the following: the nature and severity of the deficiency, the amount of time normally needed to correct such a deficiency, the availability of resources to correct the deficiency, and the vessel's itinerary.
 - a. Security-Related Deficiencies. Compliance dates for security-related discrepancies will normally require a more stringent timeline for correction than safety-related discrepancies. In addition, vessel control actions should be considered a tool to ensure compliance prior to vessel departure or next U.S. port call.
 - b. Safety-Related Deficiencies. For most safety-related discrepancies, a one-month compliance date will be appropriate.
3. Deficiency Format: Deficiencies should be written as described in the *Port State Control Job Aid*; see Appendix 1 or <http://www.uscg.mil/hq/g-m/pscweb/index.htm>. International convention cites shall be used on foreign vessels, when applicable.

ENCLOSURE 3
BOARDING PROCEDURES

BOARDING PROCEDURES

This enclosure details the guidelines and procedures for vessel boardings.

ENCLOSURE 3 - **Introduction**

1. Types of Boarding Exams
2. Authority

A. Table 3-1: Boarding Decision/Boarding Location Reference Table for Vessels Arriving or In a U.S. Port

B. Security Boarding Procedures

1. Purpose
2. Authority
3. Discussion
4. Procedures

C. Security Compliance Examination Procedures: *ISPS/MTSA Security Compliance Examination and Non-Convention Vessel Security Compliance Examination*

1. Purpose
2. Applicability
3. Definitions
4. General
5. *ISPS/MTSA Security Compliance Examination Procedures at Sea*
6. *ISPS/MTSA Security Compliance Examination in Port*
7. *Non-Convention Vessel Security Compliance Examination*

D. Safety Compliance Examination Procedures: *Port State Control (PSC) Safety and Environmental Protection Compliance Examination*

1. Purpose
2. Authority
3. Procedures

Introduction

This enclosure explains examination and boarding procedures as specified in laws, convention agreements, and regulations that apply to all foreign vessels operating in U.S. waters.

1. Types of Boarding Examinations

United States Coast Guard (USCG) examinations and boardings performed on board foreign vessels involve a combination of law enforcement and safety and security verification procedures authorized by an array of legal authorities. Whether a vessel is a high interest vessel (HIV) or a vessel selected for examination for any other reason, one, some, or all of the following boarding examinations may be appropriate:

The *Port State Control (PSC) Safety and Environmental Protection Compliance Examination* looks at how vessels comply with safety and environmental protection regulations and conventions. The decision to complete this exam is based on the outcome of an unclassified screening called the *PSC Safety and Environmental Protection Compliance Targeting Matrix*.

The *ISPS/MTSA Security Compliance Examination* looks at how vessels comply security regulations and conventions. The decision to complete this exam is based on the outcome of an unclassified screening called the *ISPS/MTSA Security Compliance Targeting Matrix*.

Since there are some vessels that need to comply with domestic regulations, but not international conventions, the *Non-Convention Vessel Security Compliance Examination* was needed. (For example, vessels subject to the Caribbean Cargo Ship Safety Code need to comply with regulations issued under MTSA, but not with SOLAS conventions and the ISPS Code.) The *Non-Convention Vessel Security Compliance Examination* looks at how vessels comply domestic security regulations. The decision to complete this exam is based on the outcome of an unclassified screening called the *ISPS/MTSA Security Compliance Targeting Matrix*.

A “security boarding” is different than the *ISPS/MTSA Security Compliance Examination* and the *Non-Convention Vessel Security Compliance Examination*. Rather than examining a vessel for compliance to regulations or conventions, the purpose of a security boarding is to enforce laws. Thus, a security boarding is not considered one of the *Compliance Verification Examination Matrices*. The decision to make a security boarding is based on the outcome of a classified screening called the *Security Boarding Decision Matrix*.

Please see Enclosure 1 of this NVIC for more information on the screening tools, collectively referred to as the *Compliance Verification Examination Matrices: PSC Safety and Environmental Protection Compliance Targeting Matrix., ISPS/MTSA Security Compliance Targeting Matrix, or the Security Boarding Decision Matrix*.

For vessels boarded prior to port entry, the Captain of the Port (COTP) boarding team ensures each vessel selected for boarding meets certain minimum standards to transit a port. Meeting these standards thus ensure that the vessel poses neither a risk to security, nor a threat to the safety of the port, the environment, or the vessel's crew.

2. Authority

When a COTP boarding team conducts a *Non-Convention Vessel Security Compliance Examination*, the team is functioning under the authority of several United States (U.S.) laws and regulations that specifically address customs, immigration, and security matters. Included among them are 50 United States Code (USC) 191, 14 USC 89, 33 USC 1226 and 33 Code of Federal Register (CFR) Part 6.

When a team is conducting a *ISPS/MTSA Security Compliance Examination* or *Non-Convention Vessel Security Compliance Examination*, authority is provided under the International Convention of Safety of Life at Sea (SOLAS), Chapter XI-2, and domestic regulations issued under the Maritime Transportation Security Act of 2002 (MTSA). Regulations issued under MTSA include 33 CFR Parts 101-106.

When a team is conducting a *PSC Safety and Environmental Protection Compliance Examination*, authority is provided under 14 USC 89(a), SOLAS, the International Convention for the Prevention of Pollution from Ships (MARPOL) 73/78, 33 CFR 164, the International Convention on Standards of Training, Certification and Watchkeeping, 1978 (STCW) 95, as well as others that address material safety issues and crew training.

A. Boarding Decision/Location Reference Table for Vessels Arriving or In a U.S. Port

Each Notice of Arrival (NOA) received by a COTP leads to the use of a screening tool. These tools use a process known as Risk-Based Decision Making (RBDM) to determine the threat a vessel poses to a U.S. port. These RBDM tools, collectively referred to as the *Compliance Verification Examination Matrices*, will prioritize vessel boardings. The *Compliance Verification Examination Matrices* will also determine what type of boarding will occur and where the vessel will be boarded. The table below describes the boarding requirement for each designation assigned to each vessel entering a U. S. port.

Table 3-1 Boarding Decision/Boarding Location Reference Table (See Note 1)

	PI	PII	PIII
ISPS I	<p><u>Board:</u> at sea <u>Conduct:</u></p> <ul style="list-style-type: none"> • <i>MTSA/ISPS Security Compliance Exam</i> • <i>PSC Safety/Environmental Compliance Exam</i> <p>(See Notes 2 & 11)</p>	<p><u>Board:</u> at sea <u>Conduct:</u> <i>MTSA/ISPS Security Compliance Exam</i></p> <p><u>Board:</u> in port <u>Conduct:</u> <i>PSC Safety/Environmental Compliance Exam</i></p> <p>(See Notes 3 & 11)</p>	<p><u>Board:</u> at sea <u>Conduct:</u> <i>MTSA/ISPS Security Compliance Exam</i></p> <p><u>IF RANDOMLY SELECTED</u> <u>Board:</u> in port <u>Conduct:</u> <i>PSC Safety/Environmental Compliance Exam</i></p> <p>(See Notes 4 & 11)</p>
ISPS II	<p><u>Board:</u> in port <u>Conduct:</u> <i>MTSA/ISPS Security Compliance Exam</i></p> <p><u>Board:</u> at sea <u>Conduct:</u> <i>PSC Safety/Environmental Compliance Exam</i></p> <p>(See Notes 5 & 11)</p>	<p><u>Board:</u> in port <u>Conduct:</u></p> <ul style="list-style-type: none"> • <i>MTSA/ISPS Security Compliance Exam</i> • <i>PSC Safety/Environmental Compliance Exam</i> <p>(See Note 6)</p>	<p><u>Board:</u> in port <u>Conduct:</u> <i>MTSA/ISPS Security Compliance Exam</i></p> <p><u>IF RANDOMLY SELECTED</u> <u>Board:</u> in port <u>Conduct:</u> <i>PSC Safety/Environmental Compliance Exam</i></p> <p>(See Note 7)</p>
ISPS III	<p><u>Board:</u> at sea <u>Conduct:</u> <i>PSC Safety/Environmental Compliance Exam</i></p> <p><u>IF RANDOMLY SELECTED</u> <u>Board:</u> in port <u>Conduct:</u> <i>MTSA/ISPS Security Compliance Exam</i></p> <p>(See Notes 8 & 11)</p>	<p><u>Board:</u> in port <u>Conduct:</u> <i>PSC Safety/Environmental Compliance Exam</i></p> <p><u>IF RANDOMLY SELECTED</u> <u>Board:</u> in port <u>Conduct:</u> <i>MTSA/ISPS Security Compliance Exam</i></p> <p>(See Note 9)</p>	<p><u>IF RANDOMLY SELECTED</u> <u>Board:</u> in port <u>Conduct:</u></p> <ul style="list-style-type: none"> • <i>MTSA/ISPS Security Compliance Exam</i> • <i>PSC Safety/Environmental Compliance Exam</i> <p>(See Note 10)</p>

Notes to Table A-1:

Note 1: This table does not address HIVs. Vessels designated by the COTP as HIVs will be boarded at sea in accordance with the requirements of section B of this enclosure.

Note 2: A vessel designated as ISPS I/PI must be boarded at sea to conduct a *MTSA/ISPS Security Compliance Examination* and a *PSC Safety and Environmental Protection Compliance Examination*. The *MTSA/ISPS Security Compliance Examination* will include verification that the vessel's security program conforms to requirements issued under MTSA. Certain elements of the *MTSA/ISPS Security Compliance Examination*, such as procedures for cargo handling, stores handling and access control, may be completed once the vessel arrives in port.

Note 3: A vessel designated as ISPS I/PII must be boarded at sea to conduct an *MTSA/ISPS Security Compliance Examination*. The *MTSA/ISPS Security Compliance Examination* will include verification that

Enclosure (3) to NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 06-03

the vessel's security program conforms to requirements issued under MTSA. Certain elements of the *MTSA/ISPS Security Compliance Examination*, such as procedures for cargo handling, stores handling and access control, may be completed once the vessel arrives in port. A *PSC Safety and Environmental Protection Compliance Examination* may be completed in conjunction with the *MTSA/ISPS Security Compliance Examination* or may be conducted pier-side, prior to cargo operations or passenger embarkation/debarkation.

Note 4: A vessel designated as ISPS I/PIII must be boarded at sea to conduct an *MTSA/ISPS Security Compliance Examination*. The *MTSA/ISPS Security Compliance Examination* will include verification that the vessel's security program conforms to requirements issued under MTSA. Certain elements of the *MTSA/ISPS Security Compliance Examination*, such as procedures for cargo handling, stores handling and access control, may be completed once the vessel arrives in port. A *PSC Safety and Environmental Protection Compliance Examination* is not required; however, if randomly selected, a *PSC Safety and Environmental Protection Compliance Examination* will also be conducted. Whether the *PSC Safety and Environmental Protection Compliance Examination* takes place at sea or in port is at the discretion of the COTP.

Note 5: A vessel designated as ISPS II/PI will be boarded at sea to conduct a *PSC Safety and Environmental Protection Compliance Examination* and boarded in port to conduct an *MTSA/ISPS Security Compliance Examination*. The *PSC Safety and Environmental Protection Compliance Examination* will include verification that the vessel security program conforms to the ISPS Code and regulations issued under MTSA. Certain elements of the *MTSA/ISPS Security Compliance Examination* may be completed once the vessel arrives in port.

Note 6: A vessel designated as ISPSII/PII will be boarded in port to conduct an *MTSA/ISPS Security Compliance Examination* and a *PSC Safety and Environmental Protection Compliance Examination* prior to any vessel operations. The *MTSA/ISPS Security Compliance Examination* will include verification that the vessel's security program conforms to requirements issued under MTSA. Certain elements of the *MTSA/ISPS Security Compliance Examination*, such as procedures for cargo handling, stores handling and access control, may be completed after commencing cargo operations.

Note 7: A vessel designated as ISPS II/PIII will be boarded in port to conduct an *MTSA/ISPS Security Compliance Examination*. The *MTSA/ISPS Security Compliance Examination* will include verification that the vessel's security program conforms to requirements issued under MTSA. A *PSC Safety and Environmental Protection Compliance Examination* is not required; however, if randomly selected, a *PSC Safety and Environmental Protection Compliance Examination* will also be conducted. Whether this examination is conducted at sea or in port is at the discretion of the COTP.

Note 8: A vessel designated as ISPS III/PI will be boarded at sea to conduct a *PSC Safety and Environmental Protection Compliance Examination*. If randomly selected for *MTSA/ISPS Security Compliance Examination*, this examination may be conducted in port. Any *MTSA/ISPS Security Compliance Examination* will also include verification that the vessel's security program conforms to requirements issued under the MTSA.

Note 9: A vessel designated as ISPSIII/PII will be boarded in port to conduct a *PSC Safety and Environmental Protection Compliance Examination* prior to any vessel operations. If randomly selected for *MTSA/ISPS Security Compliance Examination*, this examination may be conducted in port. Any *MTSA/ISPS Security Compliance Examination* will also include verification that the vessel security program conforms to requirements issued MTSA.

Note 10: A vessel designated as ISPS III/PIII requires neither a *MTSA/ISPS Security Compliance Examination* nor a *PSC Safety and Environmental Protection Compliance Examination*. If randomly selected for *MTSA/ISPS Security Compliance Examination* or *PSC Safety and Environmental Protection Compliance Examination*, the examination(s) may be conducted in port. Any *MTSA/ISPS Security Compliance Examination* will also include verification that the vessel's security program conforms to requirements issued under MTSA.

Note 11: Where the table below refers to an “at-sea” boarding location should be designated by the COTP. The COTP should consider local geography, the safety and security of the port, space for maneuvering, and safety of personnel during at-sea transfers when designating the at-sea boarding area.

Notwithstanding the above, certain vessels may be designated HIV by the COTP, and these will be boarded at sea.

The *Compliance Verification Examination Matrices* apply to vessels in port and to those arriving. If a vessel experiences a situational change, such as a change of flag State, the matrices should be reapplied to determine whether a change in boarding priority is indicated. For example, a vessel not designated as HIV prior to port entry may be redesignated HIV when in port and a HIV boarding should be conducted as soon as possible, but no later than vessel’s departure.

B. Security Boarding Procedures

1. Purpose: A security boarding, as defined in Chapter 10 of the Maritime Law Enforcement Manual (MLEM) COMDTINST M16247.1 (series) is an examination by an boarding team of a vessel (including the cargo, documentation, and persons on board) designated by the COTP, arriving or departing at a U.S. port, to deter acts of terrorism and/or transportation security incidents.
2. Authority: The principal source of Coast Guard authority for this boarding is 14 USC 89(a). This law allows Coast Guard personnel to board any vessel in U.S. waters, including foreign-flag vessels, to enforce U.S. laws and regulations, to examine and search vessels, and, when necessary, arrest individuals in violation of those laws and regulations. Reference should be made to Chapter 2 of the MLEM for a detailed discussion of this authority.
3. Boarding Procedures. Security boardings are law enforcement in nature and should be conducted in accordance with the policy and procedures outlined in the MLEM. Chapters 1 through 4 of the MLEM, contains overarching policy regarding the conduct of MLE operations, including a law and policy framework, policy on the conduct of boarding operations and rules governing the use of force. Chapter 10 of the MLEM further discusses policy and procedures for conducting security boardings. Boarding team members should be qualified in accordance with the MLEM. Exceptions to arming team members or removal of law enforcement equipment should comply with Chapter 3 of the MLEM. A qualified marine inspector or port State control officer (PSCO) will also attend each security boarding, and should hold a relevant qualification. For example, if the boarding team will be boarding a tank vessel, then the Marine Inspector should hold a tank vessel inspection qualification. The primary responsibility of this individual is to assist the boarding officer (BO) in identifying shipboard hazards as well as using the Inspector’s knowledge to confirm the vessel’s declared intent. Generally, in this context, the BO is the lead person on the boarding team

4. Discussion: Each security boarding should involve observation, inspection, and verification of the following:
 - a. Observation of the vessel prior to boarding,
 - b. Verification of the information submitted in the NOA and collection of information intended to assist the COTP in deciding whether to permit the vessel to enter or leave port,
 - c. Verification that the vessel and crew are operating in a manner consistent with the stated purpose of the vessel's intended arrival,
 - d. Clarify, verify, and act on any intelligence that may have prompted the security boarding or HIV designation.

These tasks are completed through examination of cargo, documentation, and persons on board, focusing on the deterrence of acts of terrorism and/or transportation security incidents (as defined in 46 USC 70101 (6)).

The security boarding will take place prior to any other vessel-related activity. This includes, but is not limited to, other Federal and State agency actions, vessel replenishment activity, and cargo operations. However, pilot boarding may be permitted.

5. Procedures:
 - a. Prior to commencing a security boarding, the boarding team should meet to review pertinent vessel information and discuss the boarding plan. The vessel information to be reviewed should include the NOA, Vessel Critical Profile, safety concerns, cargo information, and number of crewmembers and passengers. All planning for transportation, boarding team composition, and other related issues is the responsibility of the cognizant COTP.
 - b. If arriving at the vessel by waterborne transport while the vessel is underway or anchored, the boarding team should circle the vessel to gain a general overview of the vessel's material condition and understanding of the vessel's structure. Also, the boarding team should observe the vessel's identification number at this time to ensure the information is consistent with the NOA.
 - c. Upon embarkation, the boarding team will briefly meet with the vessel's master and ship security officer (SSO) or vessel security officer (VSO) to outline the procedures and requirements of the boarding. If a pilot is already on board, meet with this individual to determine if any unusual or suspicious activities have occurred since the pilot's arrival.
 - d. Immediately upon completion of this meeting, the boarding team should conduct the remainder of the boarding in accordance with the procedures outlined in Chapter 3 of

the MLEM. The Basic Initial Safety Inspection (BISI) should be conducted as outlined in Chapter 3 of the MLEM.

- e. Upon the completion of the BISI, boarding team will use available resources to determine the intent of the vessel during its time visiting the port, and examine all items that could cause damage to the U.S., its people or its possessions. At a minimum, the following areas of the vessel will be examined:
 - (1) NOA and Document Check: Through reviews of the vessel's particulars, interviews of various crewmembers, ship's logs, and bills of lading, verify that the information supplied in the NOA is correct. Review the Safety Management Certificate and Document of Compliance. Ensure these are valid and that required examinations and surveys have been conducted and recorded. Dangerous Cargo Manifest (DCM): Certify that the DCM contains the required information. Verify document's accuracy when conducting the deck walk.
 - (2) Crewmember Identification: Certify that only crewmembers listed on the Crew List supplied to the National Vessel Movement Center (NVMC) are on board. Certify that the information provided on the NVMC Crew List is correct by comparing it with the mariners passport and merchant mariner's credentials. At the same time, verify that the vessel's manning meets that required by the Regulations by crosschecking the Safe Manning Document, the Crew List, and mariner's STCW credentials.
 - (3) Passenger Identification: For cargo vessels certificated to carry 12 or fewer passengers, certify that the only passengers on board are those listed on the Passenger List supplied to the National Vessel Movement Center (NVMC). Certify that the information provided on the NVMC Passenger List is correct by reviewing passports. Do not attempt this check on cruise ships!
 - (4) Ship's Log: Review the ship's log for entries indicating that pre-entering port tests were performed as required by 33 CFR 164. Also, verify that the list of previous ports provided in NOA matches logbook entries.
 - (5) General safety/security: Team members should maintain vigilance throughout the boarding to ensure that any safety hazards that might exist do not affect security or safety. A qualified marine inspector will also attend the security boarding to verify the vessel is in good material condition and will not create a safety risk to the port. Any discrepancies noted should be reported to the BO or the PSCO, or both. In this context, however, the BO is generally the lead person on the boarding team.
- f. The International Ship & Port Facility Security (ISPS) Code plays a significant role in establishing whether security measures are in place on board a vessel. Certain elements of the ISPS Code assist in determining the security risk that a vessel poses to the

U.S. These items should also be examined and reviewed as part of every *ISPS/MTSA Security Compliance Examination*, discussed in more detail in Part C of this enclosure. Brief descriptions of ISPS Code elements that should be examined during this boarding are as follows:

- (1) Determine the security level at which the vessel is operating. The ship security level must be at least as high as that set at the intended port of call. If the ship is at a lower security level than the port, the ship must take steps to set its security level at least as high as that set at the arrival port;
 - (2) Verify the International Ship Security Certificate (ISSC) is on board and valid. The ISSC, if current, is considered valid unless there is evidence or reliable information that the vessel is not in compliance with the requirements of SOLAS Chapter XI-2 and the ISPS Code. Refer to Enclosure 3, Part C for a detailed discussion regarding the validity of the ISSC.
 - (3) Review the Continuous Synopsis Record (CSR). The BO should bring a copy of the information supplied in the NOA and review the CSR to verify that the CSR information matches the NOA information. While verifying this information, the BO should check similar information on other documents, such as Passenger Ship Safety Certificate, International Oil Pollution Prevention Certificate, and Cargo Ship Safety Construction Certificate, to ensure consistency with the CSR.
 - (4) Review the records of security threats, incidents, and breaches to determine if any security-related incidents have occurred in the vessel's recent history. If so, the BO should determine the details of the incident in order to assess whether this is relevant to the current port visit or poses any potential threat that the incident may have to the vessel's current security posture.
 - (5) Verify that the Ship Hull Identification Number is permanently marked and matches that listed on the ISSC. (Note - this may be done immediately prior to boarding as described above).
- g. Should the boarding team discover information that the vessel should not be permitted to transit port, or if the team notes a deficiency in the vessel's security program, they should immediately advise the COTP. The COTP should evaluate the specifics of the situation and exercise appropriate control actions to mitigate any risk posed by the vessel. Appropriate control measures may include: delaying the vessel, detention of the vessel, restriction of operations, including movement within the port, expulsion of the vessel from port, or denial of entry to the port. Depending on the discrepancy, the authority for taking control actions may involve a COTP order or a SOLAS control measure. Refer to the procedures regarding Control and Enforcement (Enclosure 4).
- h. Vessels that have been denied entry or otherwise required to depart U.S. waters as a result of security-related discrepancies may be targeted for future security boardings

or *ISPS/MTSA Security Compliance Examinations* or both at sea prior to any subsequent U.S. port entry.

C. Security Compliance Examination Procedures: ISPS/MTSA Security Compliance Examination and Non-Convention Vessel Security Compliance Examination

1. Purpose: Amendments to SOLAS Chapter V and XI, including SOLAS Chapter XI-2, were adopted on December 12, 2002, in order to prevent and suppress terrorism against ships, improve security aboard and ashore, and reduce the risk to passengers, crew, and port personnel on board ships and in port areas, for vessels and their cargoes. SOLAS Chapter XI-2 provides the special measures to enhance maritime security including, the obligations and requirements for ships, port facilities, companies, vessel masters, flag Administrations, and port States relating to security. It also establishes related control and compliance measures. The ISPS Code was also adopted on that date and provides implementing requirements and guidance for SOLAS Chapter XI-2. The ISPS Code was developed to establish an international framework involving cooperation between Contracting Governments, Government agencies, local administrations, and the shipping and port industries to detect security threats and take preventative measures against security incidents affecting ships and port facilities used in international trade. The ISPS Code establishes the respective roles and responsibilities of the Contracting Governments, Government agencies, local administrations, and the shipping and port industries at the national and international level for ensuring maritime security. Lastly, the ISPS Code provides requirements to ensure early and efficient collection and exchange of security-related information, methodology for security assessments so as to have in place plans and procedures to react to changing security levels, and confidence that adequate and proportionate maritime security control measures are in place. Foreign vessels that visit the U.S. that are subject to the requirements of SOLAS Chapter XI-2 and the ISPS Code will be examined for compliance with the requirements of these international maritime security standards.

Regulations authorized under the Maritime Transportation and Security Act of 2002 (MTSA) also apply to certain foreign vessels calling at U.S. ports. The stated purpose of these regulations is to align, where appropriate, the requirements of the domestic maritime security regulations with the international maritime security standards of SOLAS Chapter XI-2 and the ISPS Code, Parts A and B. Foreign vessels subject to SOLAS Conventions that have on board a valid ISSC that certifies the verifications required by the ISPS Code, Part A, Section 19.1 have been completed will be deemed in compliance with the regulations provided the additional requirements of 33 CFR Sections 104.240, 104.255, 104.292, and 104.295, as applicable, are met. Foreign vessels not subject to SOLAS conventions that meet regulatory applicability must comply with the regulations as discussed herein. Furthermore, provisions of MTSA also subject vessels that arrive from ports not maintaining adequate antiterrorism measures to additional conditions of entry.

2. Applicability:
 - a. The ISPS Code applies to the following ships engaged on an international voyage:

- (1) Passenger ships, including high-speed passenger craft;
- (2) Cargo ships, including high-speed craft, of 500 gross tons and greater;
- (3) Mobile offshore drilling units (MODU's – see definition in Chapter XI-2, Regulation 3)

The ISPS Code also applies to those port facilities that serve the above listed ships.

- b. The regulations implementing MTSA apply to the following foreign ships engaged on international voyages:
 - (1) MODU, cargo, or passenger vessel subject to SOLAS Chapter XI (same as 2.a.1 through 2.a.3 above)
 - (2) Foreign cargo vessel greater than 100 gross register tons (see definition in 33 CFR 101.105)
 - (3) All vessels arriving from ports not maintaining antiterrorism measures.
3. Definitions: Refer to the definitions contained in SOLAS Chapter XI-2, Regulation 1, ISPS Code Part A, Section 2, and ISPS Code Part B Section 2
4. General: Since 1994, the PSC program has had a dramatic influence upon the elimination of substandard shipping. This program now includes changes that integrate verification and enforcement of the provisions of SOLAS Chapter XI-2, the ISPS Code, and MTSA into the existing PSC structure and processes.

PSC for maritime security relies upon several elements to ensure vessels not in compliance with international safety and security standards do not enter or pose a hazard to the U.S. These elements focus on poor performance of owners, operators, charterers, flag Administrations, and recognized security organizations (RSO) that Administrations may authorize to act on their behalf. This is done through: risk-based screening of vessels; on board verification of potentially noncompliant vessels; and enforcement actions that may include, among other actions, denial of entry, detention, or ordering a vessel out of port.

To meet port State responsibilities for vessels selected for maritime security compliance examination, Marine Inspectors and PSCOs must verify that the vessels and their crews are in compliance with international conventions and U.S. laws related to security. The Marine Inspectors and PSCOs, based on their observations and questioning of the vessel's crew, must determine the depth and scope of the examination. The intent is to verify that the ship has an acceptable security program in place and that the flag Administration or authorized RSO has performed appropriate verifications and audits of the vessel's security program.

The items discussed in Section C below are an extensive list of possible examination items related to security equipment, operations, security plans, and records. This listing is intended to assist USCG PSCOs in performing examinations of foreign-flag vessels

subject to MTSA, SOLAS Chapter XI-2, and the ISPS Code. It is not the USCG's intention to inspect all the items discussed in Section C below at every exam; rather the PSCO should refer to the various items that may be examined during an *ISPS/MTSA Security Compliance Examination* and how to perform examinations of particular items. As always, the inspector's experience, knowledge, and judgment will determine the depth and scope of each examination.

The ISPS Code is separated into two parts. Part A includes the mandatory requirements of the Code for both vessels and facilities. Part B offers guidance for the implementation of these mandatory requirements. Throughout Part A of the Code, requirements refer to "taking into account the guidance or relevant provisions of Part B of the Code". Wherever this language occurs, the entity that invokes a requirement for which Part B guidance applies must fully take into account the relevant provisions of Part B to comply with the Part A requirement. The PSCO will take the guidance provided in Part B of the ISPS Code into account when performing an *ISPS/MTSA Security Compliance Examination*.

For example, in Paragraph 9.4 of Part A, "such a [ship security] plan shall be developed, taking into account the guidance given in Part B of the Code ...". Paragraph 9.9 of Part B provides that the SSP should establish the security measures covering all means of access to the ship and Paragraph 9.14 through 9.17 provides guidance on appropriate access control measures for security levels 1, 2, and 3. The U.S. will expect that the ship has security measures in place, which conform to the applicable guidance given in these Part B Paragraphs, and any evidence or reliable information that this guidance has not been taken into account may constitute grounds for control and compliance measures.

5. *ISPS/MTSA Security Compliance Examination Procedures at Sea*: A foreign vessel that has on board a valid ISSC that attests to the vessel's compliance with SOLAS Chapter XI-2 and the ISPS Code, Part A, having taken into account the relevant provisions in the ISPS Code, Part B is deemed to be in compliance with MTSA regulations, except for additional requirements in Title 33 CFR 104.240 (Maritime Security Level coordination and implementation), 104.255 (Declaration of Security), 104.292 (Additional requirements – passenger ships and ferries), and 104.295 (Additional requirements – cruise ships), as applicable. Those ships selected for an at-sea *ISPS/MTSA Security Compliance Examination* will be examined for compliance with SOLAS maritime security requirements as follows:
 - a. Determine the security level at which the vessel is operating. The ship security level must be at least as high as that set at the intended port of call. If the ship is at a lower security level than the port, the ship must take steps to set its security level at least as high as that set at the arrival port. For compliance verification, the PSCO should compare the port security level with that reported by the ship. After this check, the PSCO should judge the security posture of the vessel and whether this is consistent with the appropriate security measures expected for the port's security level. For example, a vessel at security level 1 would be expected to screen or search all unaccompanied baggage, whereas at security level 2 the vessel would be expected to

subject all such baggage to x-ray examination. To accomplish this, the PSCO should develop a competency in recognizing security enhancements that apply at security levels 2 and 3.

- b. If the vessel has arrived from a port that does not maintain adequate antiterrorism measures, determine the security level that the maintained at that port. If the vessel did not maintain at least security level 2, additional PSC measures should be considered as outlined in Enclosure 4 of this NVIC.
- c. Verify the ISSC is on board and valid. SOLAS Chapter X1-2, Part A, Section 19.2 requires that each passenger vessel, cargo vessel, including high-speed craft, of 500 gross tons or greater, and MODU engaged on an international voyage, shall be issued an ISSC. The PSCO should verify the ISSC is on board the vessel, is properly endorsed by the flag Administration or RSO, and is valid. If the ship has an interim ISSC, confirm that the conditions for interim certification outlined in Section 19.4.2 of ISPS Code, Part A, are satisfied.
- d. Verify Ship Security Performance: The flag Administration, or an RSO on behalf of the flag Administration, should approve the SSP. The SSP should be on board the vessel or kept in an electronic format, and protected from unauthorized disclosure. For at-sea boardings, PSCO's should verify that the SSP is on board the vessel. The SSP should be written in the working language, or languages, of the crew, and, if this language is not English, French or Spanish, a translation into one of these languages should be available. **The SSP is not generally subject to inspection;** however, the PSCO should, through observation, asking questions and reviewing security records, determine whether there are non-conformities related to vessel security. If there are clear grounds for believing that the ship does not have required security procedures in place, or is otherwise in violation of security provisions that should be specified in the SSP, PSCO's should examine the relevant sections of the plan. Before doing so, the PSCO must obtain the consent of either the vessel's flag State, or the master of the vessel as specified in Paragraph 9.8.1 of ISPS Code Part A **Note, the security provisions addressed in Paragraph 9.4, subparagraphs .2, .4, .5, .7, .15, .17, and .18 of Part A of the ISPS Code, may not be reviewed without the consent of vessel's flag State.**

The following is a discussion of each of the required elements of a SSP per Section 9.4 of ISPS Code Part A and the PSCO's verification procedures for each:

- (1) * *Measures designated to prevent weapons, dangerous substances and devices intended for use against people, ships or ports from being carried on board the vessel.* The PSCO should observe procedures in place to determine whether security personnel are screening persons, packages, baggage, and stores to ensure weapons, dangerous substances and devices are not brought on board and whether security personnel show competence in these duties. The PSCO

* PSCOs should defer the items noted with an asterisk to when the vessel is in port so that direct observations of security procedures and competence of crew in these procedures may be performed.

should ask security personnel tasked with these duties related questions such as, “*How do you screen carry on baggage and persons coming on board from bringing on board unauthorized weapons?*” or “*How do you intensify such screening as the security level (or MARSEC level) increases from security level 1 to 2 or from level 2 to 3?*” or “*How do you segregate checked persons and their personal effects from unchecked persons and their personal effects?*” For cruise ships, the PSCO should also verify that the vessel meets the screening requirements contained in 33 CFR 104.295, which requires screening of **all** persons, baggage and personal effects at all MARSEC levels. Additional guidance regarding this required element may be found in the ISPS Code, part B, section 9.

- (2) *Identification of the restricted areas on board the vessel and measures for the prevention of unauthorized access to the ship and to restricted areas.* The PSCO should observe whether effective access control procedures, such as locks or guards, are in place for key spaces on board the ship including, but not limited to, the bridge, steering gear compartment, engine room, cargo control spaces, communications rooms, and similar spaces. The PSCO should ask security personnel tasked with these duties related questions, such as, “*What methods do you use to prevent unauthorized individuals from accessing restricted areas such as the bridge, main engine room, steering compartment, cargo areas, and other control stations?*” or “*How do you intensify actions to prevent unauthorized access to restricted areas as the security level (or MARSEC level) increases from security level 1 to 2 or from level 2 to 3?*” or “*Does the ship use surveillance equipment in restricted areas and is this equipment continuously monitored?*” For passenger vessels and ferries, the PSCO should verify that the vessel meets the applicable requirements related to security sweeps prior to getting underway contained in 33 CFR 104.292. For cruise ships, the PSCO should verify that the vessel meets the applicable requirements related to security patrols and searching selected areas prior to embarking passengers and sailing contained in 33 CFR 104.295.
- (3) * *Measures for the prevention of unauthorized access to the ship.* The PSCO should observe that access control procedures are in place at all potential vessel accesses, that persons coming on board the vessel are screened and that the security personnel performing access control duties are knowledgeable. The PSCO should observe that crew with access control duties closely examine personal identification for validity and determine whether persons seeking to come on board have lawful business to come on board the vessel. The PSCO should ask security personnel related questions to determine their familiarity with access control procedures, such as, “*How do you identify persons coming on board and ensure they have a valid reason for being on board?*” or “*How do you intensify such screening activities related to personal identification and*

* PSCOs should defer the items noted with an asterisk to when the vessel is in port so that direct observations of security procedures and competence of crew in these procedures may be performed.

valid reason to be on board as the security level (or MARSEC level) increases from security level 1 to 2 or from level 2 to 3?” or “Have you identified the access points to the vessel when it is moored and how do you protect these areas against unauthorized access?” For passenger vessels and cruise ships, the PSCO should verify that the vessel meets the applicable requirements for the related to screening of persons contained in 33 CFR 104.292 and 104.295 which discuss security sweeps of vessels if left unattended, identification checks and confirmation of reasons for coming on board and alternatives to identification checks and passenger screening.

- (4) *Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operation of the ship or ship/port interface.* The PSCO should ask security personnel with duties related to security response related questions, such as, *“Do you have procedures in place for security threats including bomb threats, unauthorized attempts to access the ship or its restricted areas, sabotage, or terrorist or criminal activity?”* and *“What, for example, is supposed to happen if someone attempted to gain unauthorized access to the bridge?”* or *“If a breach of security occurs during passenger embarkation, what procedures are in place to continue or suspend such operations?”*
- (5) *Procedures for responding to any security instruction a Contracting Government may give at security level 3.* The security program of the vessel must address security procedures that are always in place regardless of security level, including security level 1. Additional or enhanced security procedures are required at security (or MARSEC) levels 2 and 3. The PSCO should ask security personnel with duties related to increasing security posture related questions, such as, *“Do you have procedures in place to quickly respond to changes in security (or MARSEC) levels mandated by governments of ports at which the ship calls?”* and *“Could you provide some examples?”* Also, 33 CFR 104.240 mandates additional requirements including: ship notification to COTP when the ship has achieved a mandated MARSEC level; timeliness requirements for achieving mandated MARSEC levels; notification and approval procedures for entering port when mandated MARSEC levels have not been achieved; and additional physical security measures vessels must provide when the port is at MARSEC level 3. If the port is at security level 3, the PSCO should verify that the ship has complied with each security instruction (or MARSEC Directive) issued and these additional security measures.
- (6) * *Procedures for evacuation in case of security threats or breaches of security.* The PSCO should ask security personnel with duties related to evacuation

* PSCOs should defer the items noted with an asterisk to when the vessel is in port so that direct observations of security procedures and competence of crew in these procedures may be performed.

related questions, such as, “*Do you have procedures in place to evacuate the vessel if the magnitude of a security breach or threat justifies this action?*”, “*If so, how do you ensure passengers or visitors are accounted for?*” and “*How do you interface with the port facility and contracting government during such an incident?*”

- (7) * *Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects.* The PSCO should observe security personnel in the performance of their duties related to access to the ship by ship’s personnel, passengers, visitors, contractors, delivery persons; control of restricted areas of the ship; handling of cargo, handling of ship’s stores; handling unaccompanied baggage; and monitoring the security of the ship to make a general determination regarding the competence of security personnel. The PSCO should ask security personnel questions that specifically relate to their security duties, such as “*When was the last time you participated in a security drill?*”, “*What were your responsibilities during the drill?*”, “*What are your responsibilities regarding (select one or more of the following: access control, screening baggage, safeguarding restricted areas, auditing the SSP, monitoring deck areas, etc.)?*” For personnel not having specific security duties, The PSCO should limit questions to what these personnel do during security incidents, such as “*What is your responsibility if there is a security incident on board?*” The PSCO should ask similar questions to the SSO, and other questions regarding the specific SSO duties as outlined in ISPS Code, Part A, Section 12.2 on the following issues:

- (a) regular security inspections
- (b) maintaining and supervising implementation of the SSP
- (c) coordinating security aspects handling of cargo and ship’s stores
- (d) proposing modifications to the SSP
- (e) reporting deficiencies and nonconformities to the Company Security Officer (CSO)
- (f) enhancing security awareness and vigilance on board
- (g) ensuring adequate training for crew
- (h) reporting all security incidents
- (i) coordination of the SSP with the CSO and the port facility
- (j) security equipment maintenance, testing, and calibration.

- (8) *Procedures for auditing the security activities.* The PSCO should ask the SSO questions concerning frequency and procedures for SSP auditing, such as, “*What are the basic steps for performing an audit of the security procedures?*”, and “*How often do you audit ship security procedures and are there instances that would cause you to review a specific security procedure?*” The PSCO should also review vessel records pertaining to audits of security procedures to ensure these are being performed.

* PSCOs should defer the items noted with an asterisk to when the vessel is in port so that direct observations of security procedures and competence of crew in these procedures may be performed.

- (9) *Procedures for training and exercises and drills associated with the plan.* The PSCO should review security records related to security training, drills, and exercises to ensure that records are being kept and that drills are being conducted periodically as required by the ISPS Code. In addition, The PSCO should ask the SSO questions related to training, drills, and exercises such as “*How often do you perform security drills?*”, “*Could you describe the last security drill in which you participated?*”, or “*Do you have any requirements for on board security training?*”.
- (10) * *Procedures for interfacing with port facility security activities.* The PSCO should observe security procedures in place relative to the ship-to-ship or ship-to-port-facility interface. The PSCO should ask if the ship has executed a Declaration of Security with the port facility or another ship (Note: Check 33 CFR 104.255 to see whether a Declaration of Security (DoS) is required for the vessel) and review this if a DoS is in place. Further, the PSCO should ask to see any DoS executed by the ship in any of its last ten port calls (refer to SOLAS Chapter XI-2, Reg. 9.2.3). The PSCO should verify that the provisions outlined in a current DoS are being followed. The PSCO should also ask the SSO questions related to procedures for interfacing with port facility security activities, such as “*Does the ship have a process for receiving information from Contracting Governments requiring them to execute a DoS with a port facility, and if so, please elaborate?*” or “*Does the ship have a process in place to execute a DoS with a port facility, and if so, please elaborate?*”
- (11) *Procedures for the periodically reviewing and updating the SSP.* The PSCO should review security records related to SSP updates to ensure that security reviews are being conducted. In addition, The PSCO should ask the SSO questions related to periodic SSP review, such as “*Does the ship have a process for conducting periodic review of the SSP, and if so, please elaborate?*”
- (12) *Procedures for reporting security incidents.* The PSCO should also review security records to ensure these are updated to include a history of security incidents and related communications. The PSCO should ask security personnel questions related to reporting specific types of security incidents, such as “*Does the ship have procedures for reporting security incidents, and if so, please elaborate?*” or “*Has there been a recent security incident on board the vessel and, if so, what happened, what action did the ship take, and did these actions conform to the SSP?*”
- (13) *Identification of the SSO.* Soon after arrival on board, the PSCO should identify the SSO.

* PSCOs should defer the items noted with an asterisk to when the vessel is in port so that direct observations of security procedures and competence of crew in these procedures may be performed.

- (14) *Identification of the CSO including 24-hour contact details.* The PSCO should ask the SSO regarding the name and contact information for the CSO.
 - (15) *Procedures to ensure the inspection, testing, calibration and maintenance of any security equipment provided on board and frequency for testing and calibration.* The PSCO should review security records related to inspection, testing and calibration of security equipment and frequency of related actions to ensure that these are being conducted. The PSCO should examine any security equipment observed on board for material condition. In addition, The PSCO should ask the SSO questions related to inspection, testing, calibration, and maintenance of security equipment, such as “Do you have any security equipment on board that requires periodic maintenance, calibration or testing and, if so, please elaborate?”
 - (16) *Identification of the locations where the ship security alert system activation points are fitted.* The PSCO should attempt to observe security alert activation points on board the vessel. One of these must be located on the vessel’s bridge. The PSCO may **not** ask vessel security personnel where the activation points are located unless there is evidence or reliable information (for example a anonymous report from a crewmember) that this required system has not been installed.
 - (17) *Procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting.* The PSCO should also ask the SSO how the system works. Do not test this system unless:
 - (a) there is evidence or reliable information that this system is not operational and
 - (b) the competent Authority designated by the Administration (see SOLAS Chapter XI-2, Reg. 6.2) is aware of and acknowledges the test beforehand.
- e. Review the CSR. The PSCO should bring a copy of the information supplied in the NOA and review the CSR to verify the CSR information matches the NOA information. While verifying this information, the PSCO should check similar on the other documents, such as Passenger Ship Safety Certificate, International Oil Pollution Prevention Certificate, and Cargo Ship Safety Construction Certificate, to ensure consistency with the CSR.
- f. Records: Vessels should keep security records outlined below on board for a period specified by the Contracting Government (at last the last ten port calls). The PSCO should request to view these records as a verification that the vessel’s security program meets specified security requirements. The PSCO should note that records may be kept in paper or electronic format. These records should be protected against unauthorized disclosure.

* PSCOs should defer the items noted with an asterisk to when the vessel is in port so that direct observations of security procedures and competence of crew in these procedures may be performed.

- (1) Training, drills, and exercises: Vessels should keep records of the date, description of the on-board training, drill or exercise conducted, and a list of participants. (The PSCO should note that records are not required for off-ship training provided to crew. Competence of crew in security duties, and related responsibilities, is a more appropriate measure that personnel have received appropriate training.) ISPS Code, Part A Section 13.4 requires security drills at appropriate intervals. (Note: Section 13.6 of the ISPS Code, Part B, recommends that security drills be conducted at least quarterly and in circumstances in which more than 25% of the crew has changed at any one time, with personnel that have not previously participated in a drill on that ship within the past three months). The PSCO should require security drills if there is evidence or reliable information that the vessel has failed to meet its periodic drill requirement.
 - (2) Reports of security incidents: Vessels should keep records of the date, time, location, and a description of the incident, and the associated ship's response.
 - (3) Reports of security breaches: Vessels should keep records of the date, time, location, and a description of the breach, and the associated ship's response.
 - (4) Changes in security levels: Vessels should keep records of the date, time, and location of the ship, and a description of changes to the vessel's security level.
 - (5) Communications relating to the direct security of the ship: At a minimum, vessels should keep records of all communications pertaining directly to the security of the ship. Communications include reports made to Contracting Governments and flag States concerning security threats and breaches, security instructions received by the ship from Contracting Governments and flag States, and any responses acknowledging such instructions. The PSCO should examine any report of security incidents and breaches and should find associated records of security communications. Similarly, The PSCO should examine records of changes in security levels, and should find associated records.
 - (6) Internal audits and reviews of security activities: Vessels should keep records of audit and review dates, and the results of such audits and reviews.
 - (7) Periodic review of the ship security assessments: Vessels should keep records of the date periodic reviews were conducted, and the results of such reviews.
 - (8) Periodic review of the SSP: Vessels should keep records of the date of periodic reviews, and the results of such reviews should be kept. The SSP should be reviewed on an annual basis.
 - (9) Implementation of any amendments to the SSP: Once an amendment to the SSP has been approved by the Administration, these should be put in place. Documentation of such approvals should be maintained on board and the PSCO should review such documentation. These records should include installation records of new security equipment installed after issuance of the original ISSC.
 - (10) Maintenance, calibration and testing of security equipment: Vessels should keep records of the date and description of all maintenance, calibration, and tests of security equipment.
- g. Manning: In establishing the minimum safe manning level of a ship the flag Administration should take into account the manning level of the ship such that

persons with responsibilities for safe navigation of the vessel are not tasked with extensive security-related responsibilities. The PSCO should be sensitive to manning on board the ship to ensure it is safely and effectively manned for both navigation responsibilities and security responsibilities. The PSCO should be satisfied that the crew work and rest hours established in STCW Chapter VIII are being met by the manning level set by the Administration. For further guidance, refer to the ISPS Code, Part B, Section 4.28.

6. ISPS/MTSA Security Compliance Examination Procedures in Port: A foreign vessel that has on board a valid ISSC that attests to the vessel's compliance with SOLAS Chapter XI-2 and the ISPS Code, Part A, having taken into account the relevant provisions in the ISPS Code, Part B are deemed to be in compliance with the MTSA regulations, except for 33 CFR 104.240, 104.255, 104.292, and 104.295, as applicable. Ships selected for verification with SOLAS maritime security requirements will be examined as follows:
 - a. Determine the security level at which the vessel is operating. The ship security level must be at least as high as that set at the intended port of call. If the ship is at a lower security level than the port, the ship must take steps to set its security level at least as high as that set at the arrival port. For compliance verification, the PSCO should compare the port security level with that reported by the ship. After this check, the PSCO should judge the security posture of the vessel and whether this is consistent with the appropriate security measures expected for the port's security level. For example, a vessel at security level 1 would be expected to screen or search all unaccompanied baggage, whereas at security level 2 the vessel would be expected to subject all such baggage to x-ray examination. To accomplish this, the PSCO should develop a competency in recognizing security enhancements that apply at security levels 2 and 3.
 - b. If the vessel has arrived from a port that does not maintain adequate antiterrorism measures, determine the security level that the maintained at that port. If the vessel did not maintain at least security level 2, additional PSC measures should be considered as outlined in Enclosure 4 of this NVIC.
 - c. Verify that the ISSC is on board and valid. SOLAS Chapter XI-2, Part A, Section 19.2 requires that each passenger vessel, cargo vessels, including high-speed craft, of 500 gross tons or greater, and MODUs engaged on an international voyage, should be issued an ISSC. The PSCO should verify this ISSC Certificate is on board the vessel, is properly endorsed by the flag Administration or RSO, and is valid. If the ship has an interim ISSC, confirm that the conditions for interim certification outlined in Section 19.2 of ISPS Code, Part A, are satisfied.
 - d. Verify Ship Security Performance: The flag Administration, or an RSO on behalf of the flag Administration, should approve the SSP. The SSP should be on board the vessel or kept in an electronic format, and protected from unauthorized disclosure. For at-sea boardings, PSCO's should verify that the SSP is on board the vessel. The SSP should be written in the working language, or languages, of the crew, and, if this

language is not English, French or Spanish, a translation into one of these languages should be available. **The SSP is not generally subject to inspection;** however, the PSCO should, through observation, asking questions and reviewing security records, determine whether there are non-conformities related to vessel security. If there are clear grounds for believing that the ship does not have required security procedures in place, or is otherwise in violation of security provisions that should be specified in the SSP, PSCO's should examine the relevant sections of the SSP. Before doing so, the PSCO must obtain the consent of either the vessel's flag State, or the master of the vessel as specified in Paragraph 9.8.1 of ISPS Code Part A **Note, the security provisions addressed in Paragraph 9.4, subparagraphs .2, .4, .5, .7, .15, .17, and .18 of Part A of the ISPS Code, may not be reviewed without the consent of vessel's flag State.**

The following is a discussion of each of the required elements of a SSP per Section 9.4 of ISPS Code Part A and the PSCO's verification procedures for each:

- (1) *Measures designated to prevent weapons, dangerous substances and devices intended for use against people, ships or ports from being carried on board the vessel.* The PSCO should observe procedures in place to determine whether security personnel are screening persons, packages, baggage, and stores to ensure weapons, dangerous substances and devices are not brought on board and whether security personnel show competence in these duties. The PSCO should ask security personnel tasked with these duties related questions such as, "How do you screen carry on baggage and persons coming on board from bringing on board unauthorized weapons?" or "How do you intensify such screening as the security level (or MARSEC level) increases from security level 1 to 2 or from level 2 to 3?" or "How do you segregate checked persons and their personal effects from unchecked persons and their personal effects?" For cruise ships, the PSCO should also verify that the vessel meets the screening requirements contained in 33 CFR 104.295, which requires screening of **all** persons, baggage, and personal effects at all MARSEC Levels. Additional guidance regarding this required element may be found in the ISPS Code, Part B, Sections 9.
- (2) *Identification of the restricted areas on board the vessel and measures for the prevention of unauthorized access to the ship and to restricted areas.* The PSCO should observe whether effective access control procedures, such as locks or guards, are in place for key spaces on board the ship including, but not limited to, the bridge, steering gear compartment, engine room, cargo control spaces, communications rooms, and similar spaces. The PSCO should ask security personnel tasked with these duties related questions, such as, "What methods do you use to prevent unauthorized individuals from accessing restricted areas such as the bridge, main engine room, steering compartment, cargo areas, and other control stations?" or "How do you intensify actions to prevent unauthorized access to restricted areas as the security level (or MARSEC level) increases from security level 1 to 2 or from level 2 to 3?" or

“Does the ship use surveillance equipment in restricted areas and is this equipment continuously monitored?”. For passenger vessels and ferries, the PSCO should verify that the vessel meets the applicable requirements related to security sweeps prior to getting underway contained in 33 CFR 104.292. For cruise ships, the PSCO should verify that the vessel meets the applicable requirements related to security patrols and searching selected areas prior to embarking passengers and sailing contained in 33 CFR 104.295.

- (3) *Measures for the prevention of unauthorized access to the ship.* The PSCO should observe that access control procedures are in place at all potential vessel accesses, that persons coming on board the vessel are screened and that the security personnel performing access control duties are knowledgeable. The PSCO should observe that crew with access control duties closely examine personal identification for validity and determine whether persons seeking to come on board have lawful business to come on board the vessel. The PSCO should ask security personnel related questions to determine their familiarity with access control procedures, such as, *“How do you identify persons coming on board and ensure they have a valid reason for being on board?”* or *“How do you intensify such screening activities related to personal identification and valid reason to be on board as the security level (or MARSEC level) increases from security level 1 to 2 or from level 2 to 3?”* or *“Have you identified the access points to the vessel when it is moored and how do you protect these areas against unauthorized access?”*. For passenger vessels and cruise ships, the PSCO should verify that the vessel meets the applicable requirements for the related to screening of persons contained in 33 CFR 104.292 and 104.295 which discuss security sweeps of vessels if left unattended, identification checks, and confirmation of reasons for coming on board and alternatives to identification checks and passenger screening.
- (4) *Procedures for responding to security threats or breaches of security, including provisions for maintaining critical operation of the ship or ship/port interface.* The PSCO should ask security personnel with duties related to security response related questions, such as, *“Do you have procedures in place for security threats including bomb threats, unauthorized attempts to access the ship or its restricted areas, sabotage, or terrorist or criminal activity?”* and *“What, for example, is supposed to happen if someone attempted to gain unauthorized access to the bridge?”* or *“If a breach of security occurs during passenger embarkation, what procedures are in place to continue or suspend such operations?”*
- (5) *Procedures for responding to any security instruction a Contracting Government may give at security level 3.* The security program of the vessel must address security procedures that are always in place regardless of security level, including security level 1. Additional or enhanced security procedures are required at security (or MARSEC) levels 2 and 3. The PSCO should ask security personnel with duties related to increasing security posture related

questions, such as, “*Do you have procedures in place to quickly respond to changes in security (or MARSEC) levels mandated by governments of ports at which the ship calls?*” and “*Could you provide some examples?*” Also, 33 CFR 104.240 provides additional requirements including: ship notification to COTP when the ship has achieved a mandated MARSEC Level; timeliness requirements for achieving mandated MARSEC Levels; notification and approval procedures for entering port when mandated MARSEC Levels have not been achieved; and additional physical security measures vessels must provide when the port is at MARSEC Level 3. If the port is at security level 3, the PSCO should verify that the ship has complied with each security instruction (or MARSEC Directive) issued and these additional security measures.

- (6) *Procedures for evacuation in case of security threats or breaches of security.* The PSCO should ask security personnel with duties related to evacuation and related questions, such as, “*Do you have procedures in place to evacuate the vessel if the magnitude of a security breach or threat justifies this action?*”, “*If so, how do you ensure passengers or visitors are accounted for?*” and “*How do you interface with the port facility and contracting government during such an incident?*”.
- (7) *Duties of shipboard personnel assigned security responsibilities and of other shipboard personnel on security aspects.* The PSCO should observe security personnel in the performance of their duties related to access to the ship by: ship’s personnel, passengers, visitors, contractors, delivery persons; control of restricted areas of the ship; handling of cargo, handling of ship’s stores; handling unaccompanied baggage; and monitoring the security of the ship to make a general determination regarding the competence of security personnel. The PSCO should ask security personnel questions that specifically relate to their security duties, such as “*When was the last time you participated in a security drill?*”, “*What were your responsibilities during the drill?*”, “*What are your responsibilities regarding (select one or more of the following: access control, screening baggage, safeguarding restricted areas, auditing the SSP, monitoring deck areas, etc.)?*” For personnel not having specific security duties, The PSCO should limit questions to what these personnel do during security incidents, such as “*What is your responsibility if there is a security incident on board?*”. The PSCO should ask similar questions to the SSO, and other questions regarding the specific SSO duties as outlined in ISPS Code, Part A, Section 12.2 on the following issues:
 - (a) regular security inspections
 - (b) maintaining and supervising implementation of the SSP
 - (c) coordinating security aspects handling of cargo and ship’s stores
 - (d) proposing modifications to the SSP
 - (e) reporting deficiencies and non-conformities to the CSO
 - (f) enhancing security awareness and vigilance on board

- (g) ensuring adequate training for crew
 - (h) reporting all security incidents
 - (i) coordination of the SSP with the CSO and the port facility
 - (j) security equipment maintenance, testing, and calibration
- (8) *Procedures for auditing the security activities.* The PSCO should ask the SSO questions concerning frequency and procedures for auditing the SSP, such as, “*What are the basic steps for performing an audit of the security procedures?*”, and “*How often do you audit ship security procedures and are there instances that would cause you to review a specific security procedure?*”. The PSCO should also review vessel records pertaining to audits of security procedures to ensure these are being performed.
- (9) *Procedures for training and exercises and drills associated with the plan.* The PSCO should review security records related to security training, drills, and exercises to ensure that records are being kept and that drills are being conducted periodically as required by the ISPS Code. In addition, The PSCO should ask the SSO questions related to training, drills, and exercises such as “*How often do you perform security drills?*”, “*Could you describe the last security drill in which you participated?*”, or “*Do you have any requirements for on board security training?*”.
- (10) *Procedures for interfacing with port facility security activities.* The PSCO should observe security procedures in place relative to the ship-to-ship or ship-to-port-facility interface. The PSCO should ask if the ship has executed a Declaration of Security (DoS) with the port facility or another vessel and review this if a DoS is in place. Further, the PSCO should ask to see any DoS executed by the ship in any of its last ten port calls (refer to SOLAS Chapter XI-2, Reg. 9.2.3). The PSCO should verify that the provisions outlined in a current DoS are being followed. The PSCO should also ask the SSO questions related to procedures for interfacing with port facility security activities, such as “*Does the ship have a process for receiving information from Contracting Governments requiring them to execute a DoS with a port facility, and if so, please elaborate?*” or “*Does the ship have a process in place to execute a DoS with a port facility, and if so, please elaborate?*”.
- (11) *Procedures for the periodically reviewing and updating the SSP.* The PSCO should review security records related to SSP updates to ensure that security reviews are being conducted. In addition, The PSCO should ask the SSO questions related to periodic SSP review, such as, “*Does the ship have a process for conducting periodic review of the SSP, and if so, please elaborate?*”
- (12) *Procedures for reporting security incidents.* The PSCO should also review security records to ensure these are updated to include a history of security incidents and related communications. The PSCO should ask security personnel questions related to reporting specific types of security incidents,

such as, “*Does the ship have procedures for reporting security incidents, and if so, please elaborate?*” or “*Has there been a recent security incident on board the vessel and, if so, what happened, what action did the ship take, and did these actions conform to the SSP?*”

- (13) *Identification of the SSO.* Soon after arrival on board, the PSCO should identify the SSO.
 - (14) *Identification of the CSO including 24-hour contact details.* The PSCO should ask the SSO regarding the name and contact information for the CSO.
 - (15) *Procedures to ensure the inspection, testing, calibration and maintenance of any security equipment provided on board and frequency for testing and calibration.* The PSCO should review security records related to inspection, testing and calibration of security equipment and frequency of related actions to ensure that these are being conducted. The PSCO should examine any security equipment observed on board for material condition. In addition, The PSCO should ask the SSO questions related to inspection, testing, calibration, and maintenance of security equipment, such as “*Do you have any security equipment on board that requires periodic maintenance, calibration or testing and, if so, please elaborate?*”
 - (16) *Identification of the locations where the ship security alert system activation points are fitted.* The PSCO should attempt to observe security alert activation points on board the vessel. One of these must be located on the vessel’s bridge. The PSCO may **not** ask vessel security personnel where the activation points are located unless there is evidence or reliable information (for example a anonymous report from a crewmember) that this required system has not been installed.
 - (17) *Procedures, instructions and guidance on the use of the ship security alert system, including the testing, activation, deactivation and resetting.* The PSCO should also ask the SSO how the system works. Do not test this system unless:
 - (a) there is evidence or reliable information that this system is not operational and
 - (b) the competent Authority designated by the Administration (see SOLAS Chapter XI-2, Reg. 6.2) is aware of and acknowledges the test beforehand.
- e. Records: Vessel owners and operators should keep security records outlined below on board for a period specified by the contracting government (at last the last ten port calls). The PSCO should request to view these records as a verification that the vessel security program meets specified security requirements. The PSCO should note that records may be kept in paper or electronic format. These records should be protected against unauthorized disclosure.
- (1) Training, drills, and exercises: Vessels should keep records of the date, description of the on-board training, drill or exercise conducted, and a list of

participants. (The PSCO should note that records are not required for off ship training provided to crew. Observed competence of crew in security duties is a more appropriate measure that personnel have received appropriate training.) ISPS Code, Part A Section 13.4 requires security drills at appropriate intervals. (Note: Section 13.6 of the ISPS Code, Part B, recommends that security drills be conducted at least quarterly and in circumstances in which more than 25% of the crew has changed at any one time, with personnel that have not previously participated in a drill on that ship within the past three months). The PSCO should require security drills if there is evidence or reliable information that the vessel has failed to meet its periodic drill requirement.

- (2) Reports of security incidents: Vessels should keep records of the date, time, location, description of the incident, and the associated ship's response.
 - (3) Reports of security breaches: Vessels should keep records of the date, time, location, description of the breach, and the associated ship's response.
 - (4) Changes in security levels: Vessels should keep records of the date, time, location of the ship, and a description of changes to the vessel's security level.
 - (5) Communications relating to the direct security of the ship: At a minimum, Vessels should keep records of all communications pertaining directly to the security of the ship. Communications include reports made to Contracting Governments and flag States concerning security threats and breaches, security instructions received by the ship from Contracting Governments and flag States, and any responses acknowledging such instructions. The PSCO should examine any report of security incidents and breaches and should find associated records of security communications, Similarly, The PSCO should examine records of changes in security levels, and should find associated records.
 - (6) Internal audits and reviews of security activities: Vessels should keep records of audit and review dates, and the results of such audits and reviews.
 - (7) Periodic review of the ship security assessments: Vessels should keep records of the date periodic reviews were conducted, and the results of such reviews.
 - (8) Periodic review of the SSP: Vessels should keep records of the date of periodic reviews, and the results of such reviews. Review of the SSP should be performed on an annual basis.
 - (9) Implementation of any amendments to the SSP: Once an amendment to the SSP has been approved by the Administration, these should be put in place. Documentation of such approvals should be maintained on board and The PSCO should review such documentation. These records should include installation records of new security equipment installed after issuance of the original ISSC.
 - (10) Maintenance, calibration and testing of security equipment: Vessels should keep records of the date and description of all maintenance, calibration, and tests of security equipment.
- f. Review the CSR. The PSCO should bring a copy of the information supplied in the NOA and review the CSR to verify that the CSR information matches the NOA information. While verifying this information, the BO should check similar on the other documents, such as Passenger Ship Safety Certificate, International Oil

Pollution Prevention Certificate, and Cargo Ship Safety Construction Certificate, to ensure consistency with the CSR.

- g. Manning: In establishing the minimum safe manning level of a ship the flag Administration should take into account the manning level of the ship such that persons with responsibilities for safe navigation of the vessel are not tasked with extensive security-related responsibilities. The PSCO should be sensitive to manning on board the ship to ensure it is safely and effectively manned for both navigation responsibilities and security responsibilities. The PSCO should be satisfied that the crew work and rest hours established in STCW Chapter VIII are being met by the manning level set by the Administration. For further guidance, refer to the ISPS Code, Part B, Section 4.28.

7. Non-Convention Vessel Security Compliance Examination. A foreign vessel that is not subject to SOLAS yet is above 100 gross register tons as defined in 33 CFR 101.105 must meet the requirements of 33 CFR 104. This includes vessel security requirements, requirements for vessel security assessments and requirements for vessel security plans (VSPs). Non-SOLAS foreign commercial vessels selected for a *Non-Convention Vessel Security Compliance Examination* will be examined for compliance with applicable maritime security requirements as follows:

- a. Determine the security level at which the vessel is operating. The ship security level must be at least as high as that set at the intended port of call. If the ship is at a lower security level than the port, the ship must take steps to set its security level at least as high as that set at the arrival port. For compliance verification, the PSCO should compare the port security level with that reported by the ship. After this check, the PSCO should judge the security posture of the vessel and whether this is consistent with the appropriate security measures expected for the port's security level. For example, a vessel at security level 1 would be expected to screen or search all unaccompanied baggage, whereas at security level 2 the vessel would be expected to subject all such baggage to x-ray examination. To accomplish this, the PSCO should develop a competency in recognizing security enhancements that apply at security levels 2 and 3.
- b. VSP: Non-SOLAS foreign commercial vessels subject to MTSA should have USCG-approved VSPs that meet the requirements of 33 CFR 104.405. As an equivalent, these vessels may have an alternative security program (ASP), approved by the USCG, as discussed in 33 CFR 104.120(a)(3) and 33 CFR 104.140. The vessel must have on board documentation attesting to USCG approval of its SSP, or ASP, as applicable. This would generally be in the form of a plan review approval letter from the Marine Safety Center, or in the case of an ASP, an approval letter from Commandant (G-MP). Since the VSP is a Coast Guard-approved document, the PSCO may ask to look at the VSP when necessary to verify on board security processes. During each *Non-Convention Vessel Security Compliance Examination*, the following items will be examined to ensure that vessel owners, operators, and crew conform to domestic security guidelines:

- (1) *Security Organization of the Vessel:* The PSCO should examine the security organization for the vessel specified in the VSP and then confirm that ship's personnel have been assigned security duties as specified in the VSP. The PSCO should identify the VSO, the CSO's (or designated alternates) contact information, and shipboard personnel with security duties.

- (2) *Personnel Training:* The PSCO should briefly review the section of the VSP relating to security training. If the VSP specifies training requirements, the PSCO should confirm these that the specified requirements are met. The PSCO should observe security personnel in the performance of their duties related to access to the ship by ship's personnel, passengers, visitors, contractors, delivery persons; control of restricted areas of the ship; handling of cargo; handling of ship's stores; handling unaccompanied baggage; and monitoring the security of the ship to make a general determination regarding the competence of security personnel. The PSCO should ask security personnel questions that specifically relate to their security duties, such as "*When was the last time you participated in a security drill?*", "*What were your responsibilities during the drill?*", "*What are your responsibilities regarding (select one or more of the following: access control, screening baggage, safeguarding restricted areas, auditing the security VSP, monitoring deck areas, etc.)?*" . For personnel not having specific security duties, the PSCO should limit questions to what these personnel do during security incidents, such as "*What is your responsibility if there is a security incident on board?*". The PSCO should ask similar questions to the SSO, and other questions regarding the specific SSO duties as outlined in ISPS Code, Part A, Section 12.2 on the following issues:
 - (a) regular security inspections
 - (b) maintaining and supervising implementation of the VSP
 - (c) coordinating security aspects handling of cargo and ship's stores
 - (d) proposing modifications to the VSP
 - (e) reporting deficiencies and non-conformities to the CSO
 - (f) enhancing security awareness and vigilance on board
 - (g) ensuring adequate training for crew
 - (h) reporting all security incidents
 - (i) coordination of the VSP with the CSO and the port facility
 - (j) security equipment maintenance, testing, and calibration.

- (3) *Drills and Exercises:* The PSCO should briefly review the section of the VSP relating to drills and exercises. If the VSP specifies drill and exercise requirements, the PSCO should confirm these that the specified requirements are met. Security drills should be conducted at least quarterly and in circumstances in which 25% of the crew has changed at any one time, with personnel that have not previously participated in a drill on that ship within the past three months. Records should be reviewed to ensure the required drills are taking place. In addition, the PSCO should ask the SSO questions related to

training, drills, and exercises such as “*How often do you perform security drills?*”, “*Could you describe the last security drill in which you participated?*”, or “*Do you have any requirements for on board security training?*”. The PSCO should require security drills if there is evidence or reliable information that the vessel has not met the periodic drill requirement. In such cases, the drill performed should be at the direction of the master and SSO, and should test a security procedure outlined in the VSP. The drill should show that measures outlined in the VSP are executed correctly, that security personnel are competent, and that the measures adequately address the stated security threat. Afterwards, the PSCO should critique the drill and discuss corrective action if necessary to correct any deficiencies noted.

(4) *Records and Documentation*: Vessel owners and operators should keep security records outlined below on board for at least two years. The PSCO should request to view these records as a verification that the VSP meets specified security requirements. The PSCO should note that records may be kept in paper or electronic format and should be protected against unauthorized disclosure.

- (a) Training, drills, and exercises: Vessels should keep records of the date, description of the on-board training, drill or exercise conducted, and a list of participants. (The PSCO should note that records are not required for off ship training provided to crew. Observed competence of crew in security duties is a more appropriate measure that personnel have received appropriate training.) ISPS Code, Part A Section 13.4 requires security drills at appropriate intervals. (Note: Section 13.6 of the ISPS Code, Part B, recommends that security drills be conducted at least quarterly and in circumstances in which more than 25% of the crew has changed at any one time, with personnel that have not previously participated in a drill on that ship within the past three months). The PSCO should require security drills if there is evidence or reliable information that the vessel has failed to meet its periodic drill requirement.
- (b) Reports of security incidents and breaches: Vessels should keep records of the date and time, location, to whom it was reported, a description of the incident, and the associated ship’s response.
- (c) Changes in MARSEC Levels: Vessels should keep records of the date, time, location of the ship, time of compliance with additional security requirements, and a description of changes to the vessel’s security level.
- (d) Reports of security threats: Vessels should keep records of the date, time, location, to whom it was reported, a description of the incident, and the associated ship’s response.
- (e) Annual review of the VSP: Vessels should keep records of the date annual reviews were conducted, and the results of such reviews.
- (f) Implementation of any amendments to the VSP: Once an amendment to the VSP has been approved by the Administration, it should be put in place. Documentation of VSP approvals should be maintained on board so that the PSCO should review them. These records should include

installation records of new security equipment installed after issuance of the original ISSC.

- (g) Declarations of Security: Manned vessels should keep on board a copy of the last 10 DoSs and a copy of each continuing DoS for at least 90 days after its effective period. The PSCO should confirm that procedures specified in any active DoS are being followed.
 - (h) Maintenance, calibration and testing of security equipment: Vessels should keep records of the date and description of all maintenance, calibration, and tests of security equipment.
- (5) *Response to Change in MARSEC Level*: The PSCO should briefly review the section of the VSP relating to changes in MARSEC level. If the port is at security level 3, the PSCO should verify that the ship has complied with each security instruction (or MARSEC Directive) issued. Further amplification on this item and additional requirements at MARSEC level 2 (equivalent to security level 2) are provided in 33 CFR 104.240.
- (6) *Procedures for Interfacing with Facilities and Other Vessels*: The PSCO should briefly review the section of the VSP relating to interfacing with facilities and other vessels. The PSCO should observe security procedures in place relative to the ship-to-ship or ship-to-port-facility interface. For example, if the ship is at a facility, the PSCO should verify that steps detailed in the VSP are being followed. The PSCO should also ask the SSO questions related to procedures for interfacing with facility security activities.
- (7) *Declarations of Security*: The PSCO should briefly review the section of the VSP relating to DoS and ask if the ship has executed a DoS with the facility and review this if a DoS is in place. The PSCO should verify that the provisions outlined in the DoS are being followed.
- (8) *Communications*: The PSCO should briefly review the section of the VSP relating to security communications. The PSCO should observe whether SSO has an effective means of communicating with vessel security personnel, and facilities interfacing with the vessel. The PSCO should also ask the SSO questions related to communications with national or local authorities with security responsibilities, such as, “*How does the flag Administration provide instructions to you concerning security levels?*”, “*What processes are in place to ensure that instructions from Governments of the countries the ship visits concerning port security levels are followed?*” or “*By what means do you communicate changes in security conditions to persons in the crew with security responsibilities?*”
- (9) *Security Systems and Equipment Maintenance*: The PSCO should review the VSP regarding actual on board security equipment and should then observe whether security systems and equipment are in good working order. The PSCO should also examine the equipment maintenance records to ensure these are

inspected, calibrated, tested, and maintained. The PSCO should also ask the SSO and persons responsible for equipment maintenance questions related to security equipment operation and maintenance, such as “*Do you have any security equipment on board that requires periodic maintenance, calibration or testing and, if so, please elaborate?*”

- (10) *Security Measures for Access Control:* The PSCO should briefly review the VSP procedures related to access control and observe whether these procedures have been implemented to determine whether security personnel are screening persons, packages, baggage, and stores to ensure weapons, and dangerous substances and devices are not brought on board and whether security personnel show competence in these duties. The PSCO should ask security personnel tasked with access control duties related questions, such as, “*How do you identify persons coming on board and ensure they have a valid reason for being on board?*” or “*How do you intensify such screening activities related to personal identification and valid reason to be on board as the security level (or MARSEC level) increases from security level 1 to 2 or from level 2 to 3?*” or “*Have you identified the access points to the vessel when it is moored and how do you protect these areas against unauthorized access?*”. For cruise ships, the PSCO should verify that the vessel meets the applicable requirements related to baggage screening contained in 33 CFR 104.295. The PSCO should observe that access control procedures are in place at all potential vessel accesses, that persons coming on board the vessel are screened and that the security personnel performing access control duties are knowledgeable. The PSCO should observe that crew with access control duties closely examine personal identification for validity and determine whether persons seeking to come on board have lawful business to come on board the vessel. The PSCO should ask security personnel related questions to determine their familiarity with access control procedures. For passenger vessels and cruise ships, the PSCO should verify that the vessel meets the applicable requirements for the related to screening of persons contained in 33 CFR 104.292 and 104.295.
- (11) *Security Measures for Restricted Areas:* The PSCO should briefly read the provisions in the VSP regarding spaces designated as restricted areas and the procedures used to safeguard these spaces from unauthorized access. The PSCO should observe whether these procedures are in place. These should include effective access control procedures, such as locks or guards, are in place for restricted areas including, but not limited to, the bridge, steering gear compartment, engine room, cargo control spaces, communications rooms, and similar spaces. The PSCO should verify whether restricted areas should be properly marked. The PSCO should ask security personnel tasked with these duties related questions, such as “*What methods do you use to prevent unauthorized individuals from accessing restricted areas such as the bridge, main engine room, steering compartment, cargo areas, and other control stations?*” or “*How do you intensify actions to prevent unauthorized access to restricted areas as the security level (or MARSEC level) increases from security*

level 1 to 2 or from level 2 to 3?” or “Does the ship use surveillance equipment in restricted areas and is this equipment continuously monitored?”. For passenger vessels and ferries, the PSCO should verify that the vessel meets the applicable requirements related to security sweeps prior to getting underway contained in 33 CFR 104.292. For cruise ships, the PSCO should verify that the vessel meets the applicable requirements related to security patrols and searching selected areas prior to embarking passengers and sailing contained in 33 CFR 104.295.

- (12) *Security Measures for Handling Cargo:* The PSCO should briefly review VSP procedures related to handling cargo. During cargo operations, The PSCO should observe whether the VSP measures related to cargo handling, such as procedures to prevent tampering, procedures to prevent unauthorized cargo from being loaded, inventory control, and checking cargo for dangerous substances are being applied. The PSCO should ask security personnel tasked with cargo handling duties related questions, such as, “*How do you deter tampering with cargo?*” or “*What procedures do you use to identify cargo to ensure it is approved for loading onto the vessel?*”
- (13) *Security Measures for Delivery of Vessel Stores and Bunkers:* The PSCO should briefly review VSP procedures related to handling ship stores and bunkers. During delivery of ships stores and bunkers, the PSCO should observe whether the VSP measures related to stores and bunker handling, such as procedures to prevent tampering, procedures to prevent unauthorized cargo from being loaded, inventory control, and checking cargo for dangerous substances are being applied. The PSCO should ask security personnel tasked with vessel stores and bunkers duties related questions, such as, “*How do you deter tampering with ship stores or bunkers?*” or “*What procedures do you use to prevent stores from being accepted unless ordered?*”
- (14) *Security Measures for Monitoring:* The PSCO should observe the on board implementation of security measures including: watchmen, deck watches, waterborne patrols, and roving patrols; lighting at vessel access points, cargo control points, and near restricted areas; and surveillance equipment. The PSCO should ask SSOs and personnel with security duties questions concerning security measures for monitoring, especially regarding increased measures for MARSEC levels 2 and 3. Such questions might include, “*What provisions are in place to continuously monitor the vessel, (or restricted areas, the area surrounding the vessel, including watersides)?*”, “*What special lighting provisions are in place to assist with access control?*”, or “*Could you describe how you step up security measures for monitoring when the vessel is at security (MARSEC) levels 2 and 3?*”
- (15) *Security Incident Procedures:* The PSCO should ask security personnel questions related to response actions and reporting specific types of security incidents, such as, ‘*Do you have procedures in place for security threats*

including bomb threats, unauthorized attempts to access the ship or its restricted areas, sabotage, or terrorist or criminal activity?” and “What, for example, is supposed to happen if someone attempted to gain unauthorized access to the bridge?” or “If a breach of security occurs during passenger embarkation, what procedures are in place to continue or suspend such operations?” The PSCO should also review security records to ensure these are updated to include a history of security incidents.

- (16) *Audits and VSP Amendments:* The PSCO should ask the SSO questions concerning frequency and procedures for *Non-Convention Vessel Security Compliance Examination* auditing and amendments. The PSCO should also review vessel records pertaining to periodic audits to ensure periodic audits are being performed. The PSCO should review security records related to VSP updates to ensure that security reviews are being conducted. In addition, The PSCO should ask the SSO questions related to periodic VSP review, such as, “*What are the basic steps for performing an audit of the security procedures?*”, and “*How often do you audit ship security procedures and are there instances that would cause you to review a specific security procedure?*”
- (17) *Vessel Security Assessment Report:* The Vessel Security Assessment Report is the foundation for the VSP and should be included as part of the VSP. The PSCO should ensure whether this report is included with the VSP.
- (18) *VSP Verification:* At the vessel’s first U.S. port visit after VSP approval, the PSCO should perform a more detailed security examination of the vessel to verify that the provisions of the approved VSP have been implemented. Similarly, at first U.S. port visits after approved modifications have been made to the VSP, the PSCO should perform a detailed examination of approved modifications to the VSP to verify that these modifications to the VSP have been implemented.

D. Safety Compliance Examination Procedures: Port State Control (PSC) Safety and Environmental Protection Compliance Examination

1. Purpose: The purpose of the U.S. PSC program is to reduce deaths, injuries, loss of damage or property, marine pollution and disruptions to maritime commerce resulting from foreign vessels.
2. Authority: PSC authority is derived from several sources, both domestic and international. A State may enact its own laws and regulations imposing requirements on foreign vessels trading in its waters (i.e., the double hull requirements imposed under the Oil Pollution Act of 1990 (OPA 90), or the navigation safety regulations found in 33 CFR part 164). In addition, States which are party to certain international conventions (i.e. SOLAS, International Convention on Load Lines 1966 (ICLL); International Convention for the Prevention of Pollution from Ships 73/78 (MARPOL); the International Convention on Standards of Training Certification and Watchkeeping for Seafarers, 1978, as amended in 1995 (STCW 95); and International Labor Organization Convention No. 147, The Convention Concerning Minimum Standards in Merchant Ships (ILO 147)) are empowered to verify that vessels of other nations operating within their waters comply with these conventions, and to take action to bring these ships into compliance if they do not.
3. Procedures: The general examination (i.e. "walk through") portion of PSC Safety and Environmental Protection Compliance Examination should be conducted with the following purposes in mind:
 - a. The ISPS Code plays a significant role in establishing whether security measures are in place on board a vessel. Certain elements of the ISPS Code assist in determining the security risk that a vessel poses to the U.S. These items should be examined and reviewed as part of every *ISPS/MTSA Security Compliance Examination*, and are discussed in more detail in Part C of this enclosure. Brief descriptions of ISPS Code elements that should be examined during this boarding are as follows:
 - (1) Determine the security level at which the vessel is operating. The ship security level must be at least as high as that set at the intended port of call. If the ship is at a lower security level than the port, the ship must take steps to set its security level at least as high as that set at the arrival port.
 - (2) Verify the ISSC is on board and valid. The ISSC, if current, is considered valid unless there is evidence or reliable information that the vessel is not in compliance with the requirements of SOLAS Chapter XI-2 and the ISPS Code. Refer to Enclosure 3, Part C for a detailed discussion regarding the validity of the ISSC.
 - (3) Review the CSR. The PSCO should bring a copy of the information supplied in the NOA and review the CSR to verify that the CSR information matches the NOA information. While verifying this information, the BO should check similar on the other documents, such as Passenger Ship Safety Certificate,

International Oil Pollution Prevention Certificate, and Cargo Ship Safety Construction Certificate, to ensure consistency with the CSR.

- (4) Review the records of security threats incidents and security breaches to determine if any security related incidents have occurred in the vessel's recent history. If so, the BO should determine the details of the incident in order to assess whether this is relevant to the current port visit or poses any potential threat that the incident may have to the vessel's current security posture.
 - (5) Verify the Ship Hull Identification number is permanently marked and matches that listed on the ISSC. Note: This may be done immediately prior to boarding as described above.
- b. Structure: The boarding team should develop an impression of shell maintenance and the general state of the deck and side shell of the vessel to determine if it is fit for service and route intended.
- (1) Deck Portion: The condition of such items as ladderways, guardrails, firemans, piping, hatch covers, watertight and weathertight closures, and deck plating should be observed. Areas of extensive corrosion or pitting should influence the decision as to whether it is necessary to make the fullest possible examination of the structure with the vessel afloat.
 - (2) Hull Portion: Significant areas of damage, cracking, wastage, corrosion, or pitting of plating and associated scantlings in decks and hull affecting material fitness or strength to take local loads may justify detention. When practical, internal structural members visible from deck in open cargo bays or upper wing tanks should be observed. The boarding team should be vigilant to evidence of improper temporary repairs, soft patches, recent welding or other hot work, and seepage from fuel, cargo, or ballast tanks and sideshell plating.
 - (3) Ballast Tank Entry: Due to concern for the personal safety of marine inspectors, entry into ballast tanks is no longer part of a *PSC Safety and Environmental Protection Compliance Examination* for chemical tankers, liquefied natural gas carriers, and liquid petroleum tankers. The policy of annual ballast tank entry and examination on foreign oil tankers over 10 years old is outlined in MSM II-D6.C.6.c.
 - (4) Load Lines: The boarding team should pay particular attention to closing appliances, the means of freeing water from the deck, and arrangements for the protection of the crew. Items such as defective hatch closing arrangements, multiple missing dogs, corroded vents, and wasted coamings may warrant further examination.
 - (5) Material condition affecting the vessels service and route intended: Damage not affecting the material condition of the vessel will not constitute grounds for

judging that a vessel should be detained, nor will damage that has been temporarily but effectively repaired for a voyage to a port for permanent repairs. However, in assessing the effect of damage, the boarding team should regard the location of crew accommodations and whether the damage substantially affects its habitability.

- (6) Voyage Damage: Voyage damage that is being properly addressed by the vessel's crew, owner, classification society or flag State without prompting from the Coast Guard should not constitute grounds for detaining a vessel. Other control measures, (i.e. requiring tug assists, daylight transits, portable pumps or generators etc.) may be imposed through a COTP Order in these cases. However, if voyage damage is not being properly addressed, or it appears that the vessel intends to depart port in a material condition affecting the vessel's service and route intended, the OCMI or COTP should consider taking immediate steps to detain the vessel. Substitution of liferafts for a damaged lifeboat (with the approval of the Flag Administration, or other organization that issued the Safety Equipment Certificate), should be evaluated to ensure that 100% of the crew will be accommodated, and that another boat (rescue or lifeboat) is available for marshalling rafts.
- c. Machinery Spaces: The boarding team should assess the condition of the machinery and the electrical installations such that they are capable of providing sufficient continuous power for propulsion and auxiliary services.
- (1) Operation: The boarding team may determine if responsible personnel are familiar with their duties related to operating machinery such as:
 - (a) Emergency and standby electrical power sources
 - (b) Auxiliary steering gear
 - (c) Bilge and fire pumps
 - (d) Any other equipment essential in emergency situations
 - (2) Maintenance: During examination of the machinery spaces, the boarding team will form an impression of the standard of maintenance. Frayed or disconnected wires, disconnected or inoperative reach rods, quick closing valves or machinery trip mechanisms, missing valve hand wheels, evidence of chronic steam, water and oil leaks, dirty tank tops and bilges, or extensive corrosion of machinery foundations are indicative of poor maintenance. A large number of temporary repairs, including pipe clips or cement boxes, indicate a reluctance to make permanent repairs.
 - (3) Tests and Trials: While it is not possible to determine the condition of the machinery without performance trials, general deficiencies such as leaking pump glands, dirty water gauge glasses, inoperable pressure gauges, rusted relief valves, inoperative or disconnected safety or control devices, evidence of repeated operation of diesel engine scavenger belt or crankcase relief valves,

malfunctioning or inoperative automatic equipment and alarm systems, and leaking boiler casings or uptakes, would warrant inspection of the engine room log book and investigation into the record of machinery failures and accidents and a request for running tests of machinery.

- (4) Oil and Oily Mixtures: By taking into account the quantity of oil residues generated, the capacity of sludge and bilge water holding tanks, the capacity of the oily water separator, and the oil record book, the boarding team may determine if reception facilities have been used and note any alleged inadequacies of such facilities.
 - (5) Sufficient Power: If one electrical generator is out of commission, the boarding team should investigate and test whether power is available to maintain essential and emergency services.
 - (6) Remote Shut-Off Valve for Tanks Less Than 500 Liters: Regulation II-2/15.2.5 of SOLAS 74 (amended) requires every fuel oil pipe from a storage, settling or daily service tank to be fitted with a means to secure flow from outside the space in which the tank is situated. The U.S. accepts the IMO interpretation of SOLAS II-2/15.2.5 that was adopted at the 69th session of the Marine Safety Committee in May 1998. Therefore, vessels with emergency generator fuel tanks installed on or after May 14, 1998, of 500 liters (0.500 cubic meters) and greater must have valves installed that meet this regulation. Existing installations with a capacity of 500-1,000 liters (0.500-1.000 cubic meters) are grandfathered.
- d. Navigation Safety Equipment Check: Determine through operator competence if all equipment was working properly during the last voyage. If equipment is not working, determine when repairs will be made. If a major piece of electronic equipment (like the radar or Automatic Radar Plotting Aid (ARPA)) is not operational, the OCMI or COTP should be contacted for instructions.

Conduct a thorough check of the bridge and navigation spaces for compliance with the Navigation Safety Regulations (33 CFR 164). Ask to have the electronic equipment operating if cargo operations permit.

Check the complete list of navigation safety items, paying special attention to the extra requirements for vessels over 10,000 gross tons. Check or test the equipment paying particular attention to the following:

- (1) Position Fixing Device (LORAN C, Satellite Navigation System (SATNAV) or GPS): Operate the equipment. Check that the receiver is able to lock on and track the signals for these readings. For SATNAV, see that the mate is able to set up the receiver to obtain the vessel's position on the next usable satellite pass.

- (2) Automatic Radar Plotting Aid (ARPA): Ensure that each vessel over 10,000 gross tons is equipped with an ARPA as required by the Port and Tanker Safety Act and the Navigation Safety Regulations. Take the time to spot targets on the screen and to follow a vessel's movement across the screen.
- (3) Echo Depth Sounder and Recorder: Operate the equipment to see if it gives a reading. The recorder will show recent performance if it was operational as the vessel entered the harbor.
- (4) Marine Radar: Operate the radar and note targets moving across the screen or pick out shore objects on the radar if possible. Check both radars on vessels over 10,000 gross tons, including true north stabilization features.
- (5) Vessel FM Radio: Ensure that the vessel has the capability to use VHF Channels 13, 16 and 22 and that the radios are in working order. A radio check is not necessary unless you suspect that the radios do not work.
- (6) Magnetic Steering Compass: Check to see if there is a current deviation table posted near the magnetic compass. The table should be derived from swinging the vessel and there should be a comparison log showing entries of the differences between the vessel's true, gyro and magnetic north compass readings. The magnetic compass can vary depending on the type of cargo loaded and it may show differences from voyage to voyage. Check the emergency steering compass periscope, if fitted, to ensure that you can see the card. Check compass illumination.
- (7) Gyrocompass: Check the reading on the steering gyrocompass against the repeaters on the bridge wings, the second steering station and the steering engine room. Be sure to ask if the gyro is operable since they are sometimes secured during an extended port stay. Look at the comparison log for any fluctuations between the gyro, magnetic and true readings.
- (8) Rudder Angle Indicator: Check the rudder angle indicator in all locations such as main steering station, bridge wings, and emergency steering station. They should all have the same reading. A few degrees variance is acceptable.
- (9) Navigation Information:
 - (a) Charts: Check charts of the areas to be transited within the COTP zone to see if they are maintained up-to-date. Use a list of the most recent Defense Mapping Agency (DMA) notice to mariners changes to verify that a chart is corrected up-to-date. Foreign charts are acceptable if they contain similar information and are of a large enough scale to permit safe navigation. NVIC 9-83 provides additional guidance regarding application of the requirements

for carriage of charts. Electronic charts are not an acceptable substitute for paper charts.

(b) Publications: Vessels must carry a currently corrected copy of, or applicable currently corrected extract from, the U.S. navigation publications (or foreign equivalents) listed in 33 CFR 164.33. Further enforcement guidance is provided in NVIC 9-83. Publications required include:

- i. U.S. Coast Pilot
- ii. Coast Guard Light List
- iii. Tide Tables
- iv. Tidal Current Tables or River Current Publication

(10) Relative Motion Plotting Equipment: While the ARPA may do some of the relative motion plotting for the vessel personnel, the vessel still must have equipment for manual plotting of relative motion. Normally this equipment consists of maneuvering boards, triangles, parallel rules, etc.

- e. Cargo Vessel Safety Construction Items: The general condition of the vessel may lead the boarding team to consider matters other than those concerned with safety equipment and assignment of load lines, but nevertheless associated with the safety of the vessel. This involves the effectiveness of items associated with the Cargo Ship Safety Construction Certificate, which can include hatch coamings and covers, pumping arrangements, means for shutting off air and oil supplies in the event of fire, alarm systems, and emergency power supplies.
- f. Cargo Ship Safety Radio Operation: The validity of the Cargo Ship Safety Radiotelegraphy, Safety Radiotelephony Certificate, or Cargo Ship Safety Radio Certificate may be accepted as proof of the provision and effectiveness of its associated equipment, but the boarding team should also ensure that appropriate certified personnel are carried for its operation and for listening periods. The radio log should be examined to confirm that mandatory safety radio watches are being maintained.
- g. Equipment in Excess of Convention or Flag State Requirements: Equipment on board that is expected to be relied on in situations affecting safety or pollution prevention must be in operating condition. If such equipment is inoperative and is in excess of the equipment required by an appropriate convention or the flag State, it should be repaired, removed or, if removal is not practicable, clearly marked as inoperative and secured.
- h. Garbage: The boarding team may determine if all operational requirements of Annex V of MARPOL 73/78 have been met. The boarding team may determine if the reception facilities have been used and note any alleged inadequacy of such facilities.

- i. Manuals and Instructions: The boarding team must determine if appropriate crewmembers understand the information given in manuals and instructions relevant to the safe condition and operation of the vessel and its equipment. They must also ensure that they are aware of requirements for maintenance, testing, training drills, and required logbook entries.

- j. STCW 95: STCW sets qualification standards for masters, officers and watch personnel on seagoing merchant ships. STCW was adopted in 1978 at the International Maritime Organization (IMO) in London, and entered into force in 1984. The Convention was significantly amended in 1995. The 133 current state-parties to the Convention represent approximately 98 percent of the world's merchant vessel tonnage. The United States became a party in 1991. The 1995 amendments greatly altered the Convention by including addressing several factors commonly discussed as the human element:
 - (1) Multinational Crews: The 1995 Amendments take into account the increasing use of multinational crews. Therefore, the responsibility for competency of crews, which once fell only on flag State administrations, is now spread over all parties that issue certificates. Under the new rules, the party issuing the original certificate must comply with the requirements of the Convention, and the flag State may issue a separate "recognition" certificate only after confirming that the original certificate was issued in accordance with the Convention. This recognition process does not affect U.S. citizens serving on U.S. vessels. U.S. mariners serving on foreign-flag vessels, however, would be affected.
 - (2) PSC: The 1995 Amendments strengthen the PSC provisions of the STCW Convention by expanding the grounds on which a foreign ship may be detained, and allowing PSCOs to look beyond merchant mariner's certificates and conduct direct assessments of the competence of merchant mariners.
 - (3) Rest Periods: To address the problem of crew fatigue, the STCW Amendments requires that every person assigned duty as an officer in charge of a watch or as a rating forming part of a watch should receive a minimum of 10 hours of rest in any 24-hour period. These 10 hours of rest may be divided into two parts as long as one segment is at least 6 hours long, with strictly limited exceptions.
 - (4) Training Requirements: The Amendments require that seafarers be provided with "familiarization training" and "basic safety training" which includes basic fire fighting, elementary first aid, personal survival techniques, and personal safety and social responsibility. This training is intended to ensure that seafarers are aware of the hazards of working on a vessel and can respond appropriately in an emergency.
 - (5) ARPA/GMDSS: The Amendments require training on use of Automatic Radar Plotting Aids (ARPA) and Global Maritime Distress Safety System (GMDSS) for deck officers serving on vessels equipped with those systems. In cases where

a vessel is not fitted with those systems, the license and STCW endorsement would state that limitation.

- (6) Bridge Teamwork Procedures: The Amendments require that the master and deck officers have a thorough understanding of bridge teamwork procedures. In the U.S., this is understood to be an ability to apply principles of bridge resource management.
- (7) Examinations and Demonstrations of Skills: The revised technical regulations specify minimum standards of competence for the range of certificates to be issued under STCW. The standards are presented in tables with four columns: a) 'competence' or ability to be established; b) area of 'knowledge, understanding and proficiency' within each competence; c) 'methods of demonstrating competence', and d) 'criteria for evaluating competence.' The Amendments also promote the use of simulators as one of the recognized means for demonstrating competence. The Coast Guard is developing standards and procedures and performance measures for use by designated examiners to evaluate competence in various areas.
- (8) Quality Standards System: STCW, as amended, requires all training and assessment activities to be "continuously monitored through a quality standards system to ensure achievement of defined objectives, including those concerning the qualifications and experience of instructors and assessors." The 1995 amendments require those responsible for instruction and assessment of the competence of seafarers to be qualified for the type and level of training or assessment involved. Persons performing these roles are expected to have received guidance in instructional techniques and assessment methods. The Coast Guard has drafted policy guidance for use in qualifying and managing training and assessment personnel.
- (9) RO-RO Passenger Ships: The 1995 Amendments included new regulations (V/2) on training and qualification for masters, officers, ratings and other personnel on Roll-on Roll-off (RO-RO) passenger vessels. These regulations were developed by the IMO as a matter of urgency following the sinking of the ferry ESTONIA. A subsequent set of amendments in 1997 adds similar regulations (V/3) on personnel serving on passenger ships other than RO-RO passenger ships. Regulations currently being developed would incorporate STCW Regulation V/3 into the U.S. licensing system to meet the requirements of the 1997 Amendments. This proposed rule would only apply to U.S. passenger ships to which SOLAS certificates are issued, that is, those on international voyages.
- (10) For specific guidance regarding enforcement and examination procedures during *PSC Safety and Environmental Protection Compliance Examinations*, refer to G-MOC Policy 02-04, "Policy for the Enforcement of the 1995

Amendments to the International Convention of Standards of Training, Certification and Watchkeeping for Seafarers, 1978, (STCW 95).”

- k. ISPS Code: The ISPS Code plays a significant role in establishing whether security measures are in place on board a vessel. Certain elements of the Code assist in determining the security risk that a vessel poses to the U. S. These items should be examined and reviewed as part of every *PSC Safety and Environmental Protection Compliance Examination*. Brief descriptions of ISPS Code elements that should be examined during this boarding are as follows:
- (1) Determine the security level at which the vessel is operating. The requirement is that the ship security level must be at least as high as that set within the port to which a vessel intends to enter. If the ship is at a lower security level than the port, with the ship still at sea, the ship must take proper steps to set its security level at least as high as that at the port the ship intends to enter;
 - (2) Verify the ISSC is on board and valid. The ISSC, if current, is considered valid unless there is evidence or reliable information that the vessel is not in compliance with the requirements of SOLAS Chapter XI-2 and the ISPS Code. Refer to Enclosure 3, Part C for a detailed discussion regarding the validity of the ISSC.
 - (3) Review the CSR. The PSCO should bring a copy of the information supplied in the NOA and review the CSR to verify the CSR information matches the NOA information. While verifying this information, the BO should check similar on the other documents, such as Passenger Ship Safety Certificate, International Oil Pollution Prevention Certificate, and Cargo Ship Safety Construction Certificate, to ensure consistency with the CSR.
 - (4) Review the records of security threats incidents and security breaches to determine if any security related incidents have occurred in the vessel’s recent history. If so, the BO should determine the details of the incident in order to assess whether this is relevant to the current port visit or poses any potential threat that the incident may have to the vessel’s current security posture.
- l. Verify the Ship Hull Identification number is permanently marked and matches that listed on the ISSC. Note: This may be done immediately prior to boarding as described above.
- m. International Safety Management (ISM): Compliance with SOLAS Chapter IX and the ISM Code became mandatory for vessels engaged on an international voyage on the following dates:
- (1) Phase I: July 1, 1998: Phase I mandates passenger ships, including passenger high-speed craft, oil tankers, chemical tankers, gas carriers, bulk carriers, and cargo high-speed craft of 500 gross tons or more.

- (2) Phase II: July 1, 2002: Phase II mandates other cargo ships and self-propelled mobile offshore drilling units (MODUs) of 500 gross tons or more.

The objectives of the ISM Code are to ensure safety at sea, prevent the occurrence of human injury or loss of life, and avoid environmental and property damage. Specifically, the ISM Code seeks to address the issues of human error and human omissions. To accomplish its objectives, the ISM Code requires owners of ships, or other organizations such as the managers, or bareboat charterers, who have assumed responsibility for ship operations, to implement SMS for their ships and companies.

Specific guidance regarding the enforcement of ISM and examination details is found within NVIC 4-98.

- n. International Labour Organization (ILO) 147: During annual examinations and reexaminations, be alert for especially hazardous or unsanitary conditions. We cannot hold other countries to the same standards we expect here in the U.S. However, we should be alert to those conditions that are blatantly unsafe. Labor or pay complaints should be brought to the attention of the Department of Labor by contacting G-MOC. Where intervention authority is lacking, local humanitarian or religious organizations (i.e. Seamen's Friends Society) may be able to assist in correcting unsanitary practices or in assisting crewmembers. See COMDINST 16711.12 for further guidance.
- o. Structural Integrity: During annual examinations and reexaminations, look for evidence of long term neglect, wastage, corrosion, cracking, pitting or casualty damage. The presence on deck of plating, sections of piping, or an excessive number of oxyacetylene tanks may indicate unauthorized repairs or other problems. Look for recent burn marks from welding particularly on the reverse slope plates of the upper wing tanks if possible. Temporary repairs including cement boxes, epoxy patches, postage stamp inserts and drill stopped cracks may indicate problems. Each situation must be evaluated to determine whether the temporary repair is adequate or whether the vessel should be detained until permanent repairs are made.
- p. Cargo Operations: During annual examinations and reexaminations, check the following:
- (1) Check containers and packaged cargo for proper marking, labeling, and placarding;
 - (2) Look for damaged or leaking cargo containers and packages, particularly forklift punctures or crushing that would indicate dropped packages;
 - (3) Look for potential ignition sources, particularly from electrical equipment, smoking violations, stowage plan and cargo segregation;

- (4) Determine if the vessel has a capacity to retain all oily waste and oily bilge slops generated while operating in U.S. waters; and
 - (5) Check to see that no oil or hazardous material is carried in prohibited spaces.
- q. Cargo Securing Manual: As of December 31, 1997 Administration approved Cargo Securing Manuals (CSM's) became mandatory under SOLAS 74, Ch. VI/5 and VII/6 for all cargo vessels engaged in international trade which are equipped with cargo securing systems or individual cargo securing arrangements. Checks of foreign flag cargo vessels for CSM's, approved by the appropriate flag Administration or by organizations designated by the flag Administration, should become a routine part of *PSC Safety and Environmental Protection Compliance Examination*. NVIC 10-97 provides more amplifying information on CSM's.

Foreign flag cargo vessels found to not have an Administration-approved CSM will be required to provide a CSM prior to the next U.S. voyage. For vessels with dangerous goods/hazardous materials cargoes already aboard, CG PSCO's will evaluate the vessels securing arrangements for the dangerous goods/hazardous materials cargoes. In cases where the dangerous goods/hazardous materials cargo securing is found insufficient, appropriate corrective action will be required as a condition for departure.

For foreign-flag vessels that return to U.S. ports without CSM's on subsequent voyages, more restrictive actions may be necessary, to include:

- (1) Detention of the vessel until the vessel's owner or operator formally establishes a reasonable timeline for submittal of a CSM to the cognizant Administration or authorized representative;
 - (2) Notification of the cognizant Administration and classification society that the vessel is in violation of SOLAS 74, Ch. VI/5 and VII/6; and
 - (3) Prevention of future cargo operations at all U.S. ports until the vessel owner or operator provides proof of compliance with SOLAS 74, Ch. VI/5 and VII/6 CSM requirements.
- r. On Deck:
- (1) Note the general condition of the fuel piping systems (including manifolds), particularly any non-permanent repairs and other irregularities;
 - (2) Check the material condition of the fuel vents (Note: There is no requirement for fuel tank vent screens on foreign vessels.);
 - (3) Examine closure mechanisms for cargo hatches, sideports, watertight doors and other openings that maintain the condition of the vessel; and

- (4) Ensure that stowage and securing arrangements for on deck containers are adequate and that cargo segregation is in compliance with 49 CFR 176.83.
- (5) Lifesaving Equipment Check: During annual examinations and reexaminations, spot-check the vessel's lifesaving equipment. Observe the condition of the lifeboats paying particular attention to the hull and davits. Liferaft stowage and missing weak links are common problems that can usually be corrected quickly without detaining the vessel. The effectiveness of lifesaving equipment depends heavily on good maintenance by the crew and their use in regular drills. The lapse of time since the last survey or Safety Equipment Certificate can be a significant factor in the degree of deterioration of equipment. Apart from failure to carry equipment required by a convention or obvious defects such as holed lifeboats, look for signs of disuse of, or obstructions to, boat launching equipment that may include paint accumulation, seizing of pivot points, absence of greasing, condition of blocks and falls, and improper lashing or stowing of deck cargo. See D5.C.7.h. for guidance on abandon ship drills.
- (6) Firefighting Equipment Check: Review the vessel's fire control plan and note the adequacy and condition of firefighting equipment. Check the fire stations to ensure that there are hoses, extinguishers, fixed CO2 systems, and other firefighting equipment on the vessel as indicated in the fire control plan and/or general arrangement plan. Examine the fire detection and sprinkler systems if applicable. During annual examinations, test the fire main and pumps by charging the system and witnessing the pressure at widely separated deck stations simultaneously. Do not spend the time to look at every station, but ensure the vessel's readiness to respond to a fire. Determine if international shore connections are provided where required. For vessels in general, the poor condition of fire mains and hydrants and the possible absence of fire hoses and extinguishers in machinery or accommodation spaces points to a need for close inspection of fire safety equipment. In addition to compliance with convention requirements, look for evidence of a higher than normal fire risk. This might be brought about by a lack of cleanliness in the machinery space that, together with significant deficiencies of fixed or portable fire extinguishing equipment, could lead to a judgment of the vessel's being substandard. PSCOs should not require servicing of hand portable extinguishers by servicing contractors unless obvious deterioration is present. A last servicing date of greater than 1 year, by itself, is not sufficient to require servicing.
 - (a) Fire Doors: The spread of fire could be accelerated if fire doors are not readily operable. Inspect doors in main zone bulkheads, stairway enclosures, and boundaries of high fire risk spaces, such as main machinery rooms and galleys, for their operability and securing arrangements. Particular attention should be paid to those retained in the open position

and those in main vertical zones that may have been compromised by construction.

- (b) Ventilation Systems: An additional hazard in the event of fire is the spread of smoke through ventilation systems. Spot checks might be made on dampers and smoke flaps to ascertain the standard of operability. Ensure that ventilation fans can be stopped from the master controls and that means are available for closing main inlets and outlets of ventilation systems.
 - (c) Escape Routes: Attention should be given to the effectiveness of escape routes by ensuring that vital doors are not maintained locked and that alleyways and stairways are not obstructed.
- (7) Pollution Prevention Equipment Check: Check for compliance with the Pollution Prevention Regulations (33 CFR 155, 156 and 159) and MARPOL Regulations (Annexes I, II and V) [See 33 CFR 151 and COMDTINST M16450.30 for further guidance]. During annual examinations, this should be an in-depth look at the vessel pollution prevention requirements including examination of fuel and lubricating oil systems, waste oil handling systems, oil or liquid hazardous material transfer procedures (as applicable), garbage handling procedures, declarations of inspection, and marine sanitation devices. At a minimum, the following should be examined:

Note: These items applicable only to vessels carrying oil or liquid hazardous material as cargo (i.e., in deep tanks) or engaged in bunkering.

- (a) Examine the small discharge containment and visually check the capacity. Have someone demonstrate the mechanical means of closing scuppers and drains in the containment, and look for the means of draining or removing discharged product from the containment;
- (b) Examine the fuel and bulk lubricating oil discharge containment. Visually check the capacity. (i.e., 1/2 barrel 300-1600 gross tons, 1 barrel over 1600 gross tons, 5 U.S. gallon portable container for 100-300 gross tons, and 100 gross tons or over if constructed before July 1974);
- (c) Examine the bilge slops piping outlet. (1,600 gross tons and above, on each side of the weather deck; below 1,600 gross tons, accessible from the weather deck) Make sure the vessel has a means to stop each discharge on the weather deck near the discharge outlet;
- (d) Ensure vessel meets requirements for ballast discharge if the vessel uses ballasted fuel tanks;

- (e) Locate the emergency shutdown system. If possible, have it activated to ensure proper operation;
 - (f) Check the vessel's required transfer communications. (Continuous two-way voice between persons-in-charge of the transfer operation.) Ensure that they are intrinsically safe;
 - (g) Visually inspect required deck lighting. Check the transfer point and transfer operation work area;
 - (h) Check the hoses. Check the hose burst pressure. The minimum design burst pressure for each hose assembly must be at least four times the sum of the pressure of the relief valve setting (or four times the maximum pump pressure when no relief valve is installed) plus the static head pressure of the transfer system, at the point where the hose is installed. Check the hose working pressure. The maximum allowable working pressure (MAWP) for each hose assembly must be more than the sum of the pressure of the relief valve setting (or the maximum pump pressure when no relief valve is installed) plus the static head pressure of the transfer system, at the point where the hose is installed. Check the hose labeling. Check to see that each hose is marked with the required information; and
 - (i) Make sure the appropriate signs are displayed. Locate the "Discharge of Plastic and Garbage Prohibited" placard.
- s. In Engine Room:
- (1) Locate the oil-water separator. Check the certification label for a Coast Guard approval number or International Maritime Organization (IMO) specification label (MARPOL 73/78);
 - (2) Check the bilge continuous monitor. Note the approval number or IMO specification label and sight the recording tape;
 - (3) Check and operationally test the discharge alarm system;
 - (4) Locate the "Discharge of Oil Prohibited" placard. It is required to be in each machinery space, bilge, and ballast pump control station;
 - (5) Verify that the vessel is equipped with an operable, U.S. Coast Guard or MARPOL IV certified marine sanitation device (MSD); and
 - (6) Check the bilges. Check for presence of oil or hazardous material and confirm structural integrity.
- t. In Cargo Control Area:

- (1) Verify that the vessel has a list of designated persons-in-charge for each type of transfer operation (fueling and each product).
 - (2) Examine in depth the bulk liquid transfer procedures. Ensure that these:
 - (a) are legibly printed in a language understood by personnel engaged in the transfer operations;
 - (b) are permanently posted or available where they can easily be seen and used by crewmembers;
 - (c) contain a list of each oil or liquid hazardous material transferred (generic name, product information, applicability of transfer procedures);
 - (d) include an accurate description of each transfer system on the vessel (including a line diagram, the location of the shutoff valves, description of and procedures for emptying the discharge containment system);
 - (e) specify number of persons required to be on duty for transfer is indicated with the duties, by title, of each person required for each transfer operation;
 - (f) include procedures and duty assignments for tending the vessels moorings during transfer;
 - (g) include procedures for operating the emergency shutdown and transfer communications, topping off tanks, ensuring that all valves used during the transfer operation are closed on completion of the operation, and reporting fuel or cargo discharges;
 - (h) include any exemptions or alternatives granted are located in the front of the transfer procedures; and
 - (i) include any amendments have been incorporated.
 - (3) Confirm that the emergency shutdown is operable from the cargo control area for bulk liquid transfer operations.
- u. Abandon Ship Drill: An abandon ship drill is to be witnessed by the boarding team during annual examinations. Muster crew at their stations. Check muster lists for accuracy. Check that lifejackets are properly donned. Determine if crew members are able to communicate with each other. Ensure that crewmembers are familiar with abandon ship procedures/duties and the proper use of ship's lifesaving equipment. Lower lifeboats, where practicable, to the embarkation deck. Conduct general examination of davits, falls, sheaves, etc. as boat is being prepared and lowered to the embarkation deck. Start lifeboat engines. Lowering of lifeboats into the water,

releasing them and exercising the crew is not required. If the PSCO feels the crew is unfamiliar with their duties or incapable of safely operating the lifesaving equipment, then the drill should be halted and the Master told to conduct training and/or additional exercises. The USCG should be recalled when they are ready to conduct a drill. During follow-up exam, PSCOs may have crew lower boats into the water, release them and exercise crew, when practicable, to ensure competency of crew. Drills are determined unsatisfactory when language barriers interfere with adequate verbal communication, or when the competency of the crew is so inadequate that the drill cannot be executed safely.

- v. Fire Drill: The PSCO should witness a fire drill and evaluate the ability of the crew to respond to emergencies. The safety officer or the officer in charge will specify the location and scope of the drill. The PSCO should determine if the drill is at sufficient scope to demonstrate crew competence. All crewmembers, except those engaged in cargo operations or on watch in machinery spaces, should participate. PSCOs should observe the alarm indication on the fire alarm panel and the responses of the vessel's officers. (A normal procedure is to send an officer or fire patrolman to investigate.) Go to the location and describe the fire situation (smoke, flames, etc.) to the investigator. Observe how the report of fire is relayed to the bridge or damage control center. At this point most vessels will sound the crew alarm to summon the firefighting parties and the remainder of the crew to their stations. PSCOs should also observe the firefighting party arriving on scene, breaking out their equipment and fighting the simulated fire. Team leaders should be giving orders as appropriate to their crews and passing word back to the bridge or damage control center on the conditions. The firefighting crews should be observed for proper donning and use of their equipment. Officers should make sure that all of the gear is compatible; e.g., the breathing apparatus can be worn with the protective suit, the helmet can be worn with the air mask, and the lifeline can be attached to breathing apparatus or belt. Merely mustering the emergency crews with their gear is NOT acceptable.

- w. Steering: Steering gear failures on all classes of foreign vessels have caused serious marine casualties and pollution incidents in U.S. waters. The PSCO should witness a steering system test. The tests should include the following:
 - (1) Operationally check the main and auxiliary steering from each remote steering gear control system and each steering position on the navigating bridge;
 - (2) Test the main steering gear from the emergency power supply;
 - (3) Check the reading on the bridge gyrocompass against the repeater in the after steering room;
 - (4) Check the rudder angle indicator in the after steering room; it should have the same reading as the indicator on the bridge;

- (5) Test each remote steering gear control system power failure alarm and each steering gear power unit failure alarm;
 - (6) Test for full movement of the rudder according to the required capabilities of the steering gear;
 - (7) Test the means of communication between the navigating bridge and the steering gear compartment;
 - (8) Visually inspect the steering gear and its connecting linkage; and
 - (9) Check for indications of potential failures involving excessive leakage of hydraulic fluid; looseness in connections, fasteners, or couplings; frayed electrical wiring or evidence of arcing; unusual noises during operation; or evidence of insufficient maintenance. Examples of the latter include makeshift repairs, painted-over lube fittings, and deficient maintenance that might adversely affect operation of the steering gear.
- x. Expanding the Examination: During any examination, the boarding team should expand their examination of a vessel if their examination establishes "clear grounds" for believing that the condition of a vessel, its equipment, or crew do not correspond substantially with the particulars of the certificates. Expanded examinations should focus on those areas where "clear grounds" have been established and should not include other areas or systems unless the general impressions or observations of the boarding team support such examination.

ENCLOSURE 4

PSC ENFORCEMENT AND CONTROL PROCEDURES

TABLE OF CONTENTS

PSC ENFORCEMENT AND CONTROL PROCEDURES

A. Enforcement

1. Philosophy
2. Provisions
 - a. International
 - b. U.S.
 - c. Applicability Table

B. Clear Grounds

1. Discussion
2. Diagram

C. Vessel Control Procedures for Security and Safety

1. Denial of Entry/Expulsion
2. IMO Reportable Detentions
3. Captain of the Port (COTP) Order
4. Customs Hold
5. Restriction of Operations/Vessel Movement
6. Delay
7. Comprehensive Security Inspection
8. Letter of Deviation
9. Flag State Notification
10. Lesser Administrative/Corrective Measures

D. Administrative Enforcement Measures (Apply to both security and safety violations)

1. Civil Penalty Adjudication
2. Civil Penalty
3. Letter of Warning
4. LOU / Surety Bond

E. Port Enforcement and Control Measures

1. Security Zone
2. Naval Vessel Protection Zone (NVPZ) and Naval Protection Order
3. Regulated Navigation Area (RNA)
4. Safety Zone
5. Special Local Regulation (SLR)

Enforcement and Control Procedures

A. Enforcement

1. Philosophy:

Substandard foreign vessels and vessels that may arrive from substandard ports continue to pose safety or security threats to U.S. ports. In response to these threats, the Coast Guard has dramatically increased foreign vessel boardings and subsequent enforcement and control actions. Proper enforcement and control procedures should be followed to ensure all maritime entities are held accountable. The focus of the Port State Control (PSC) program is the identification and subsequent notification of substandard vessels to the global community. For example, if a unit issues a vessel a COTP Order but not a formal IMO Detention, it is correcting the problem locally. However, it is not alerting the domestic and global communities that the vessel and its associated parties (flag, owner, class, etc.) may be substandard. Domestically, the Coast Guard's foreign vessel targeting matrix, which is based on historical detentions, is rendered inaccurate. Globally, substandard vessels and their associated parties are not held accountable through IMO, and therefore, they can continue to operate without any restrictions. Finally, this action can hinder the Coast Guard's ability to provide accurate statistics needed to gain congressional support for the program. This support hinges on the field's ability to maintain data integrity and quality control and to pick the correct enforcement posture in each circumstance.

2. Provisions/Authorities

Several international and U.S. provisions grant the Coast Guard the authority to enforce PSC on foreign vessels.

a. International Provisions/Authorities:

- (1) International Convention for the Safety of Life at Sea (SOLAS). SOLAS Chapter I, Regulation 19, authorizes port States to board foreign vessels to determine the validity of their SOLAS certificates. Where "clear grounds" indicate that a vessel is not in compliance with applicable requirements, the port State is authorized to take necessary steps to ensure that the vessel does not sail until it can proceed to sea, or leave the port for the purpose of proceeding to a repair yard, without danger to the vessel or persons on board.
- (2) International Ship and Port Facility Safety (ISPS) Code. SOLAS Chapter XI-2, Regulation 9, authorizes port States to board foreign vessels to determine the validity of their International Ship Security Certificate. Where "clear grounds" indicate that a vessel is not in compliance with applicable requirements, the port State is authorized

to impose any one or more of the control measures in relation to that ship including inspection of the ship, delaying the ship, detention of the ship, restriction of operations, including movement within the port, or expulsion of the ship from port, including denial of entry. The port State is also authorized to impose lesser administrative or corrective measures. Any measures imposed shall be proportionate to the security noncompliance noted. Such measures shall be reasonable and of the severity and duration necessary to rectify or mitigate the noncompliance.

- (3) International Convention on Load Lines 1966 (ICLL). ICLL Article 21(1) and (2) provide the port State with the authority to board foreign vessels to verify the validity of the vessel's certificate and to determine that the vessel is not loaded beyond its allowable limits, that the position of the load line corresponds with the certificate, and that the vessel has not been so materially altered that it is manifestly unsafe to proceed to sea without danger to human life. The port State is authorized to take control as may be necessary to ensure that the vessel does not sail until it can proceed to sea without danger to passengers or crew.
- (4) International Convention for the Prevention of Pollution from Ships (MARPOL) 73/78. Article 5(2) provides port States with the authority to inspect foreign vessels to verify the validity of the vessels' certificates. Where "clear grounds" indicate that the vessel is not in compliance with the certificates, the port State is authorized to take such steps to ensure that the vessel does not sail until it can proceed to sea without presenting unreasonable threat of harm to the marine environment.
- (5) International Convention on Standards of Training, Certification and Watchkeeping for Seafarers, 1978 as amended in 1995 (STCW 95). Ships may be detained under STCW 95 authority if the deficiencies pose a danger to persons, property or the environment. These deficiencies are described in STCW Regulation I/4. Regulation I/4 will be the only cite used if a detention is warranted.
- (6) International Labor Organization (ILO) Convention No. 147. Article 4 of ILO 147 prescribes that port States may take necessary measures to rectify any conditions on board which are clearly hazardous to safety or health. The U.S. has not enacted legislation to allow specific enforcement of this treaty. However, under the Ports and Waterways Safety Act (PWSA, specifically 33 USC 1223), a COTP may exercise control over a vessel that is not in compliance with any applicable law or treaty. When a vessel poses a serious health threat to the crew, PWSA allows a COTP to use ILO 147 as a reference to measure the threat to the port and the crew and then to take action accordingly. Additional guidance may be found in COMDTINST 16711.12.
- (7) International Safety Management Code (ISM). Ships may be detained under the ISM Code if there is an apparent breakdown in the Safety

Management System of the vessel. If this occurs, an audit should be called. If major non-conformities are discovered, then expulsion from port or denial of entry, with a ban on future entry to U.S. ports should be considered.

- b. U.S. Provisions/Authorities that are applicable to foreign-flag vessels:
- (1) Marine Transportation Security Act (MTSA) [107 P.L. 295 / 33 CFR Subchapter H]: This is the controlling authority typically associated with *security*-related COTP Orders and IMO Detentions for vessels.
 - (2) Ports and Waterways Safety Act (PWSA) [33 USC 1221 et seq/ 33 CFR 160.101]: This is the controlling authority typically associated with *safety*-related COTP Orders. It can also be used to implement VTS measures for traffic separation schemes, Regulated Navigation Areas (RNAs) or Safety Zones.
 - (3) Magnuson Act [50 USC 191/33 CFR Part 6]. This is the controlling authority typically associated with *security*-related COTP Orders. This can be used to respond to acts of terrorism against a person, vessel, or structure, or to restrict waterfront access to sensitive areas.
 - (4) 33 USC 1226 This statute, separate from Magnuson Act authority, allows the COTP to take various measures to prevent or respond to an act of terrorism against individuals, vessels, or public or commercial structures within the marine environment. These measures include, but are not limited to, security and safety zones.
 - (5) Special Local Regulations (SLR) [33 CFR 100.35]. These regulations established safety zones for scheduled events and can only be promulgated by the cognizant District Commander.
 - (6) Regulated Navigation Area (RNA) [33 USC 1231 with implementing regulations of 33 CFR Part 165]. These are safety zones established for emergency measures or unanticipated events and can only be issued by cognizant District Commander.
 - (7) Naval Vessel Protection Zone (NVPZ) [14 USC 91/33 CFR Part 165] These regulations designate a 500-yard security zone around all naval vessels greater than 100 feet in length.
 - (8) 46 USC 91: This statute requires that all vessels departing the U.S. for a foreign port and all foreign vessels departing one U.S. port for another obtain U.S. Customs clearance. To ensure monetary satisfaction or surety for civil penalties, the PWSA, at 33 USC 1232, requires Customs to withhold or revoke clearance (commonly referred to as a “Customs hold”) at the Coast Guard’s request.
 - (9) 33 CFR 164.55: This is the authority that allows the COTP to grant deviations from any rule in 33 CFR. This authority is limited to safety-related violations.

- c. The table below highlights international and domestic regulatory control instruments that can be exercised on a foreign vessel in order to ensure compliance.

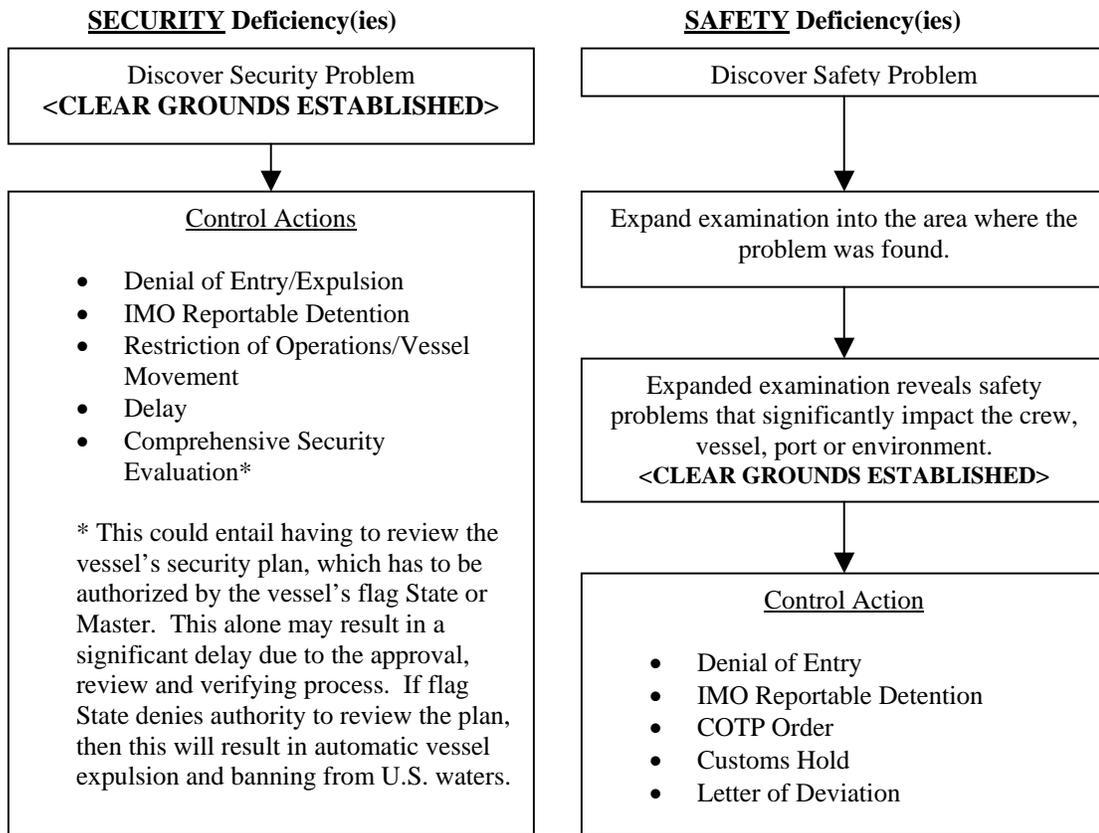
Table 4-1: Vessel Types and Regulating Provisions and Authorities

Vessel Type	SOLAS	ICLL	MARPOL	STCW 95	ILO 147	ISM Code	ISPS	MTSA
Passenger								
0 to 99 GT	X			X	X	X	X	
100 to 149 GT	X			X	X	X	X	X
150 to 399 GT	X	X		X	X	X	X	X
> 400 GT	X	X	X	X	X	X	X	X
Tank Ships								
0 to 99 GT				X	X			
100 to 149 GT				X	X			X
150 to 499 GT		X	X	X	X			X
> 500 GT	X	X	X	X	X	X	X	X
Cargo Ships								
0 to 99 GT				X	X			
100 to 149 GT				X	X			X
150 to 399 GT		X		X	X			X
400 to 499 GT		X	X	X	X			X
> 500 GT	X	X	X	X	X	X	X	X

B. Clear Grounds:

Clear Grounds means that enough information about security or safety deficiencies on a vessel has been obtained to impose appropriate control actions within U.S. waters. Clear grounds for imposing control actions under the new security regulations have a substantially lower threshold than do those for safety problems. Clear grounds are established for security control actions immediately upon discovery of a security problem. This differs from control actions for a safety deficiency, when a problem is discovered, the examination is expanded, and then control actions may or may not be taken depending on the situation. Note the difference in the clear grounds and control action thresholds with security versus safety deficiencies in Figure 4-1 below.

Figure 4-1: Thresholds for clear grounds and control actions with security versus safety deficiencies.



C. Vessel Control Procedures for Security and Safety:

The COTP shall institute appropriate control actions to safeguard the port, personnel, and the environment, when “clear grounds” have been established and/or a vessel arrives from a port that does not maintain adequate anti-terrorism measures. Such actions should be appropriate to the deficiencies. When the deficiencies do not render a vessel detainable—or, in the case of security, not subject to denial of entry or expulsion—the control actions should consider the vessel’s effort to rectify such deficiencies immediately.

1. *Denial of Entry / Expulsion:* Use this control option only when allowing a vessel into U.S. waters creates an unacceptable level of risk, which is defined as an “immediate threat” to the port, personnel or the environment. This should not be the first choice in dealing with substandard vessels and should be limited to the most egregious circumstances. In some cases, a substandard vessel may already be in U.S. waters when a PSC exam initiates an IMO detention. Some of these cases may lead to expulsion of the vessel after it has met minimum specified standards to leave port. Examples of conditions that would warrant denying a vessel entry or expulsion from port include, but are not limited, to the following:
 - a. Lack of onboard Ship Security Certificate;
 - b. Lack of an approved Ship Security Plan;
 - c. Lack of an assigned Security Officer;
 - d. Vessel Security Officer cannot display an acceptable level of competency in regards to vessel security;
 - e. Inoperable Ship Security Alert system;
 - f. Inability of crewmembers with security responsibilities to identify the locations of the Ship Security Alert system;
 - g. Arrival from a port in a country that does not maintain adequate anti-terrorism measures and refusal to comply with any additional conditions of entry as a result of an arrival from the last port of ports of call;
 - h. Submission of untimely or incomplete Notice of Arrival (NOA);
 - i. Incompatible cargoes stowed in adjacent tanks;
 - j. Cargoes being carried that are not authorized by the LOC;
 - k. Cargo leaks from tanks or piping systems;
 - l. LNG/LPG Gas detection system inoperative;
 - m. Vessel carrying cargoes not authorized to carry;
 - n. Lack of ISM Certification;
 - o. Lack of COFR;
 - p. Lack of Vessel Response Plan; and/or
 - q. IGS system deficiencies.
2. *IMO Reportable Detentions:* A vessel is deemed substandard when clear grounds that it poses an undue risk to the crew, vessel, port, or environment are discovered during a thorough PSC examination. An IMO detention should be the primary course of action when a substandard vessel should take corrective measures and the domestic and global communities should be

notified of the substandard vessel. The field's efforts to hold substandard vessels accountable will have far reaching effects, not only for the Coast Guard's PSC program but also toward meeting international expectations. Refer to Appendix A for specific examples of detainable deficiencies under their corresponding authorities.

3. Captain of the Port (COTP) Order: A COTP Order is another option to protect the safety and security of the port. An order can be used to implement a variety of control actions, including controlling the vessel's movement as it enters or departs a port or ordering the vessel out of port. The COTP/OCMI may process a civil penalty case for failure to comply with a COTP Order. A COTP Order is not a substitute for pursuing and processing a detention under the applicable provisions of SOLAS, the ISPS Code, MARPOL, and the Load Line Convention. Sample COTP orders are provided below.
 - a. Controlling the Ship's Movement. Depending on the deficiencies discovered, a COTP Order should be used to control or restrict the vessel's movement or operations. Many additional applications exist, not all of which are related to the condition of a vessel (e.g. A COTP Order may be used to order a vessel to a specific anchorage to protect a port during a hurricane.).
 - b. Controlling the Ship's Movement for Security. If there is a concern that the vessel poses a risk from sabotage or other subversive acts, a COTP Order requiring the presence of armed escort personnel onboard the vessel during the transit would be warranted.
 - c. Controlling the Ship's Movement for Safety. If the deficiency relates to the vessel's navigational equipment, the COTP Order might require an assist tug or may restrict a vessel to daylight operations. If the deficiency relates to pollution prevention equipment, the COTP Order may prohibit a vessel from bunkering or lightering until corrective measures are taken.
4. Customs Hold: Under the authority of 46 U.S.C. 91, vessels intending to depart the U.S. for a foreign port should obtain a clearance from the U.S. Customs and Border Protection (CBP). Whenever a vessel is alleged to have violated certain U.S. safety and pollution laws, the Coast Guard may request that the CBP deny or withhold the required clearance from the vessel until a bond or other surety is posted. In cases involving alleged violations of the MTSA and the proposed use of this control, the COTP should first consult with the appropriate district legal office for guidance. This control should not be relied upon when a PSC detention is the appropriate option.
5. Restrictions of Operations/Vessel Movement: Restrictions on vessel operations or movements may be imposed if vessel deficiencies pose security or safety threats. Security deficiencies on a vessel or at a facility receiving vessels that present a danger to either a vessel or facility may be addressed

one of two ways. The deficiencies may be corrected before the vessel arrives at a facility, or the vessel may be ordered to proceed to a safer location until the deficiencies are corrected. Similarly, a vessel with safety deficiencies in operations, such as cargo handling, that do not affect its fitness to proceed to sea may be ordered to correct the deficiencies. If the vessel is not restricted from departing or is not required to affect corrective measures before departure, this is not considered a detention. When the orders are given solely to comply with U.S. regulations, they should be issued under the PWSA and through a COTP Order.

6. *Delay*: Security deficiencies that should be corrected before the vessel enters port may be addressed by delaying the vessel until the deficiencies are corrected. For example, if the port is at MARSEC level 2 (generally equivalent to security level 2) and the arriving vessel is at security level 1, the ship should implement the additional security requirements of security level 2 plus the additional requirements of MARSEC level 2 before the vessel may be allowed to enter port.
7. *Comprehensive Security Inspection*: This is the minimum control action to take when clear grounds of a security deficiency have been established. Similar to the expanded exam for a safety violation, this expanded security inspection is very detailed, possibly including a review a vessel's security plan. If these plans include sensitive sections, authorization from the flag State should be obtained before this control action can be undertaken. If authorization is not obtained, the vessel should be considered for denial of entry, expulsion from port, or an IMO detention, depending on the circumstances. The prevailing need to keep U.S. ports secure justifies the potential delays to commerce that may result from this control action.
8. *Letter of Deviation*: The COTP may authorize, upon written application, a deviation from any rule in 33 CFR part 164. However, the risks imposed by equipment failures reported IAW 33 CFR 164.53, and casualties reported IAW 46 CFR 4.05, should be considered before issuing a Letter of Deviation. A boarding and examination prior to issuing a Letter of Deviation should be considered in those cases involving vessels at high risk from a safety perspective. (i.e. Priority I or II). Issuance of a Letter of Deviation does not preclude the possibility of pursuing civil penalty action. A Letter of Deviation is not an appropriate control action for security deficiencies. A sample Letter of Deviation is provided on the next page.
9. *Flag State Notification*: Whenever a foreign vessel is denied entry to a port or offshore terminal, or is detained, the unit taking that action should notify the flag State as soon as possible. Points of contact are provided on the Port State Control Website at <http://www.uscg.mil/hq/g-m/pscweb/index.htm>. IMO Assembly Resolution A.787(19), as amended by A.882(21), requires that port States initiating control actions notify the flag Administration forthwith. Further, for maritime security-related control actions, such as inspection of the

ship (as discussed in SOLAS Chapter XI-2, Reg. 9.8.1), delaying the ship, detention of the ship, restriction of operations, including movement within the port, or expulsion of the ship from the port, the unit making the control action should also notify the flag State as soon as possible. Notification should be in writing within 24 hours of initiating the action. Depending on the circumstances, flag State notification presents the best opportunity for the COTP to ask the flag Administration for permission to review relevant portions of the vessel security plan. Submittal of Forms A and B is acceptable for flag State notification; however, if such notification includes a request to review portions of the security plan, a brief letter to this effect stating the reasons such review is necessary should also be included. Should any difficulties be encountered in making this notification, contact G-MOC-2 for additional information.

10. Lesser Administrative/Corrective Measures: The COTP may choose to enforce lesser administrative or corrective measures for certain security deficiencies. For example, if a vessel is noted for non-detainable (or not subject to denial of entry or expulsion) security deficiency and it corrects the deficiency to the satisfaction of the PSCO before the vessel experiences any delay, a lesser corrective measure has occurred. Such measures are not considered reportable control actions under SOLAS Chapter XI-2 and do not need to be reported to the flag Administration.

D. Administrative Enforcement Measures (apply to both security and safety violations)

1. Civil Penalty Adjudication: Civil penalty proceedings should be initiated for all major non-criminal violations, for repeat offenses, and any minor violations that are not corrected prior to returning to a U.S. port. Penalty amounts are determined by the circumstances under which the violation occurred; seriousness of the violation; culpability of the party; prior history of similar violations, economic benefit of noncompliance to the responsible party, and the degree of success of effort by the responsible party to minimize or mitigate injury and/or risk.
2. Civil Penalty: The COTP/OCMI may process a civil penalty case for violations of U.S. laws or regulations. Civil Penalty provisions for violations of the MTSA are located in 33 CFR Subchapter H. Civil penalty enforcement should be pursued in all cases against those involved parties that are in the best position to bring about compliance and those who can best deter future violations.
3. Letter of Warning: This correspondence is appropriate for minor violations that are corrected immediately by conscientious operators. The discovery of administrative errors in dangerous cargo manifests and incorrectly sized lettering on warning signs are obvious examples of minor violations. However, a history in MISLE of continuing violations indicates the need for

more stringent enforcement actions. A Letter of Warning can be issued to all parties involved with a vessel.

4. LOU / Surety Bond: Whenever a violation case is pursued and if the law authorizing the civil penalty permits, the COTP may require a Letter of Undertaking (LOU) or Surety Bond from the vessel owner, operator, or person in charge to assure payment of any penalty or fine that may result. In cases involving an alleged violation of the MTSA, the COTP should first consult with the appropriate district legal office.

E. Port Enforcement and Control Measures

1. Security Zone: The COTP, District Commander, Area Commander, or Commandant generally establish Security zones under the authority of the Magnuson Act, 50 USC 191 and 33 CFR Part 6. Security zones may also be established under the authority of 33 USC 1226 to prevent or respond to acts of terrorism against a person, vessel, or structure. Security zones are designated areas of land, water, or land and water established for such time as the COTP deems necessary to prevent damage or injury to any vessel or waterfront facility, to safeguard ports, harbors, territories, or waters of the United States. Violations of security zones may be handled through criminal and civil penalties. COTPs may consult with their servicing legal office when establishing security zones and enforcing security zone violations.
2. Naval Vessel Protection Zone (NVPZ) and Naval Protection Order: The Atlantic Commander and the Pacific Commander under the authority of 14 USC 91 establish regulations for the protection of naval vessels. The authority to issue NVPZ is delegated from the Commandant to District Commanders and COTPs. NVPZ regulations are found in 33 CFR Part 165, Subpart G.
 - a. An NVPZ provides a 500-yard area of control around large (greater than 100 feet in length overall) U.S. naval vessels in the navigable waters of the United States. The term “naval vessel” is defined broadly to include any vessel owned, operated, chartered, or leased by the U.S. Navy, any pre-commissioned vessel under construction for the U.S. Navy, and any vessel under the operational control of the U.S. Navy or a Combatant Command. The U.S. Transportation Command, TRANSCOM, which consists of the U.S. Navy Military Sealift Command, the Army’s Military Traffic Management Command, and the Air Force’s Air Mobility Command, is a Combatant Command, as are any vessels under TRANSCOM operational control. The term naval vessel also includes floating drydocks and U.S. naval vessels in commercial drydocks within the navigable waters of the U.S., as long as all other definitional requirements are met. However, the term naval vessel does not currently include Coast Guard vessels.

- b. Within this 500-yard zone, all vessels should slow to minimum safe speed and proceed as directed by escort vessels or the naval vessel CO. Vessels with civilian masters can advertise the presence of the NVPZ but will require Navy or Coast Guard escorts, a naval officer in command, or a Coast Guard commissioned, warrant, or petty officer onboard to enforce the NVPZ. Furthermore, no vessel or person is allowed within 100 yards of a naval vessel without permission.
 - c. In addition to the Commandant's and Area Commander's authority to issue regulations, 14 U.S.C. § 91 authorizes Naval Vessel Protection Orders. The Coast Guard has not used Naval Vessel Protection Orders for some time, therefore, COTPs should contact their servicing legal office before issuing a Naval Vessel Protection Order. These orders are given to individual vessels or persons any time a specific order is necessary for the protection of a U.S. naval vessel. When necessary, a Naval Vessel Protection Order may be used to control vessels beyond the limits of the NVPZ created in 33 C.F.R. part 165 subpart G. Examples of these orders include: orders to shift anchorages, orders to proceed to a specific mooring/anchorage, to deny port entry, etc.
 - d. Naval Vessel Protection Zones can be enforced by a Coast Guard commissioned, warrant, or petty officer, or the senior naval officer present in command if the Coast Guard is not present or not present in sufficient force. Given current resource demands, it is anticipated that the USN will be responsible for enforcing these zones in many instances. Coast Guard enforcement of NVPZ's is no different from the enforcement of a safety or security zone issued under other existing authorities.
3. Regulated Navigation Area (RNA): An RNA is established by regulation and is considered a rulemaking that can be issued only by the District Commander. Whenever possible, the normal rulemaking process of notice and comment should be followed (see COMDINST M16704.2 series). However, RNAs may be established as emergency measures to respond to unanticipated events. RNAs are defined as "a water area within a defined boundary for which regulations for vessels navigating within the area have been established". RNAs are designed to define an area that requires specific control of vessel operations to preserve the safety of the adjacent waterfront structures, to ensure safe transit of vessels, or to protect the marine environment.
- a. RNAs are typically established when extensive vessel controls are needed over an extended period. They may be used to provide safety of navigation when conditions require higher standards of control and care than those provided by the Navigational Rules. They may also be used to limit activities that create an unusually high risk of harm to an environmentally sensitive area. Examples of RNAs include placing a draft restriction on an area known to have excessive, undocumented silting; establishing a

maximum speed limitation in an area known to be overly congested; and creating a no-passing or overtaking zone in an area known to have a narrow channel.

4. *Safety Zone*: The COTP or District Commander establish Safety Zones under the authority of PWSA, 33 USC 1225, as implemented by 33 CFR 165.20. Safety zones may also be established under the authority of 33 USC 1226 to prevent or respond to acts of terrorism against a person, vessel, or structure. A safety zone is a water area, shore area, or water and shore area to which, for safety or environmental purposes, access is limited to authorized persons, vehicles, or vessels. The safety zone may be stationary and described by fixed limits or may be described as a zone surrounding a vessel or facility.
5. *Special Local Regulation (SLR)*: SLRs may only be promulgated by the District Commander and are used to promote safety immediately before, during, and immediately after a “regatta or marine parade,” defined in 33 C.F.R. § 100.05 as “an organized water event of limited duration which is conducted according to a prearranged schedule.” SLRs are required by 33 C.F.R. § 100.15 for events “which by their nature, circumstances, or location will introduce extra or unusual hazards to the safety of life on the navigable waters of the United States”. Examples include inherently hazardous competitions, customary presence of marine traffic in the area of the event, and obstruction of a navigable channel that is expected to result in the accumulation of spectator craft. SLRs are published in 33 C.F.R. § 100 Subpart B. SLRs should not be used to respond to immediate threats; they are designed to afford notice and protection for recurring or pre-scheduled marine events.

APPENDIX A TO ENCLOSURE 4

EXAMPLES OF DETAINABLE DEFICIENCIES FOR SECURITY AND SAFETY

APPENDIX A

EXAMPLES OF DETAINABLE DEFICIENCIES FOR SECURITY AND SAFETY

A. DOCUMENTATION DISCREPANCIES

1. Documents not available.
2. Document missing the name of its issuing authority.
3. Document does not identify the vessel.
4. Document lacks an issue date, signature of the duly authorized official issuing the document, or seal or stamp of the issuing authority.
5. Disparities between actual condition on vessel and documentation listing.

B. INTERNATIONAL SHIP AND PORT FACILITY SAFETY (ISPS) CODE

1. Lack of or expired/invalid International Ship Security Certificate or interim International Ship Security Certificate (may deny entry/expel from port).
2. Lack of/incomplete approved ship security plan (may deny entry/expel from port).
3. Lack of an assigned ship security officer (may delay vessel).
4. Ship security officer cannot display an acceptable level of competency in regards to vessel security (may delay vessel).
5. Crew anomalies (e.g. gross incompetence, unaccounted personnel, overstaffed, fraudulent documents, etc.) (may deny entry/expel from port)
6. Evidence that vessel embarked persons or loaded stores or goods at a port facility, from another ship, or another source where these sources were not required to have an approved port facility/vessel security plan without having completed a DOS.
7. Evidence that vessel embarked persons or loaded stores or goods at a port facility, from another ship, or another source where these sources are required to have an approved port facility/vessel security plan but were in violation with SOLAS Chapter XI-2 or part A of the ISPS Code
8. Improper or incomplete Notice of Arrival information (may deny entry/expel from port).
9. Evidence or reliable information that serious deficiencies exist in the vessel's security equipment, documentation or arrangements.
10. Master or crewmembers not familiar with essential shipboard security procedures.
11. Inability of crewmembers to establish communications with other key members with security responsibilities.
12. Missing or inoperable ship security alert system.
13. Lack of Declaration of Security when required or agreed upon amongst parties (may delay vessel).
14. Evidence that cargo handling security procedures are not in place (may restrict operations).

15. Poor screening procedures associated with passenger access control or unaccompanied passenger baggage.

C. INTERNATIONAL CONVENTION OF SAFETY OF LIFE AT SEA (SOLAS)

1. Failure of proper operation of essential machinery.
2. Insufficient cleanliness of engine room.
3. Failure of proper operation of emergency generator, lighting, batteries, etc.
4. Failure of proper operation of steering gear (all modes).
5. Absence, insufficient capacity, or serious deterioration of any lifesaving appliances.
6. Absence, insufficient capacity, or serious deterioration of any firefighting appliances or fire protection (including structural).
7. Absence, substantial deterioration, or failure of proper operation of cargo deck area fire protection on tankers.
8. Absence, noncompliance, or serious deterioration of lights, shapes, or sound signals.
9. Absence or inoperable GMDSS or associated equipment.
10. Absence of non-sparking exhaust ventilation for cargo pump rooms.
11. Number, composition, or certification of crew not corresponding to safe manning document.

D. INTERNATIONAL CONVENTION ON LOADLINES (ICLL 66)

1. Significant areas of damage or corrosion, or pitting of plating affecting fitness or strength, unless proper temporary repairs for a voyage to a port for permanent repairs has been taken out.
2. A recognized case of insufficient stability.
3. Load-line violation (overloading).
4. Absence or substantial deterioration of closing devices, hatch closing arrangements, and watertight doors.

E. INTERNATIONAL CONVENTION FOR THE PREVENTION OF POLLUTION FROM SHIPS (MARPOL 73/78)

1. Absence, serious deterioration, or failure of proper operation of the oily water separator, the oil discharge monitoring and control system, or the 15-ppm alarm arrangements.
2. Remaining capacity of slop and/or sludge tank insufficient for the intended voyage.
3. Unauthorized discharge bypass fitted.

F. INTERNATIONAL CONVENTION ON STANDARDS OF TRAINING, CERTIFICATION, AND WATCHKEEPING FOR SEAFARERS (STCW)

Appendix A to Enclosure (4) to NAVIGATION AND VESSEL INSPECTION CIRCULAR NO.

1. Failure of seafarers to hold a certificate, to have an appropriate certificate, to have valid dispensation, or to provide documentary proof that an application for an endorsement has been submitted to the flag State administration.
2. Failure to comply with the applicable safe manning requirements of the flag State administration.
3. Failure of navigational or engineering watch arrangements to conform to the requirements specified by the flag State administration.
4. Absence in a watch of a person qualified to operate equipment essential to safe navigation, safety radio communications, or the prevention of marine pollution.
5. Failure to provide proof of professional proficiency for the duties assigned to seafarers for the safety of the ship and the prevention of duty.
6. Inability to provide for the first watch at the commencement of a voyage and subsequent relieving watches persons who are sufficiently rested and otherwise fit for duty.

G. INTERNATIONAL LABOUR ORGANIZATION CONVENTION NO. 147 (ILO 147)

1. Insufficient food for voyage to next port.
2. Insufficient potable water for voyage to next port.
3. Excessively unsanitary conditions on board.
4. No cooling or heating in accommodation of a ship operating in areas where temperatures may be excessive.
5. Excessive garbage, blockage by equipment or cargo or otherwise unsafe conditions in passageways/accommodations.

H. INTERNATIONAL BULK CARRIER (IBC) CODE

1. Transportation of a substance not mentioned in the Certificate of Fitness.
2. Missing or damaged high-pressure safety devices.
3. Electrical installations not intrinsically safe or corresponding to code requirements.
4. Sources of ignition in hazardous locations.
5. Insufficient heat protection for sensitive products.

I. INTERNATIONAL GAS CARRIER (IGC) CODE

1. Transport of substance not mentioned in the Certificate of Fitness.
2. Missing closing devices for accommodations or service spaces.
3. Bulkhead not gastight.
4. Defective air locks.
5. Missing or defective quick closing valves.
6. Missing or defective safety valves.

7. Electrical installations not intrinsically safe or not corresponding to code requirements.
8. Ventilators in cargo area not operable.
9. Pressure alarms for cargo tanks not operable.
10. Gas detection plant and/or toxic gas detection plant not operable.
11. Transport of substances to be inhibited without valid inhibitor certificate.

J. INTERNATIONAL SAFETY MANAGEMENT CODE (ISM) CODE

1. Safety Management Systems (SMS) documents a company's management procedures to ensure that conditions, activities and tasks, both ashore and on board, affecting safety, security and environmental protection are planned, organized, executed, and checked in accordance with statutory and company requirements. The SMS is the procedural requirements for vessels to carry out normal operations included, but not limited to, preventative maintenance, navigation procedures, bunkering operations, emergency preparedness, pollution prevention procedures, technical systems, and operations and communications procedures. With this in mind, a great deal of deficiencies can be related a failure in some standardized procedure. Therefore, if a failure occurs, the vessel and company must address it and make recommendations.
2. Should the COTP/OCMI discover vessels with failures in the vessel's SMS, the vessel should be considered for detention and an external audit requested. Should grossly negligent systems be discovered, these vessels should be considered for denial of entry until they can prove substantial compliance. Should OCMI's suspect problems exist on the company side, a letter should be forwarded to G-MOC via the district and area, fully documenting the suspected problems requesting that the flag State be urged to conduct an external audit of the company involved.

ENCLOSURE 5

GLOSSARY

GLOSSARY

ABSCONDER - An inadmissible **CREWMEMBER** that gains, or attempts to gain, illegal entry into the United States.

AGENT - A vessel representative hired by the ship's management. Ship's agents may be tasked with various jobs such as, ensuring proper vessel documentation and compliance.

AUTHORITY - The government's legal power to act.

BASELINE - The line, drawn in accordance with international law, from which the territorial sea and other maritime jurisdictional zones are measured. It is generally the low water line along the coast (including the coasts of islands) and special closing lines across the mouths of rivers, bays, inlets, and other similar indentations. Also referred to as territorial sea baseline.

BASIC INITIAL SAFETY INSPECTION (BISI) - The BISI is a quick and limited protective sweep of a vessel for boarding team safety. The scope of the BISI is determined by the circumstances of the boarding, particularly the size, type, and condition of the vessel, the demeanor of the crew (knowledge, skill level and experience), and information available to the boarding team about potential threats or hazards aboard the vessel. Further guidance on BISI can be found in Chapter 3 of the MLEM, COMDTINST M16247.1 (series).

CARGO SHIP - Any ship that is not a passenger ship.

CERTAIN DANGEROUS CARGO (CDC) - Includes any of the following:

- Division 1.1 or 1.2 explosives as defined in 49 CFR 173.50
- Division 1.5D blasting agents for which a permit is required under 49 CFR 176.415 or, for which a permit is required as a condition of a research and special programs administration exemption
- Division 2.3 "Poisonous Gas", as listed in 49 CFR 172.101 that is also a "Material Poisonous by Inhalation" as defined in 49 CFR 171.8, and that is in a quantity in excess of 1 metric ton per vessel
- Division 5.1 oxidizing materials for which a permit is required under 49 CFR 176.415 or for which a permit is required as condition of a research and special programs administration exemption
- A liquid material that has a primary or subsidiary classification of Division 6.1 "Poisonous Material" as listed 49 CFR 172.101 that is also a "material poisonous by inhalation," as defined in 49 CFR 171.8 and that is in a bulk packaging, or that is in a quantity in excess of 20 metric tons per vessel when not in a bulk packaging.
- Class 7, "Highway Route Controlled Quantity" radioactive material or "Fissile Material, Controlled Shipment," as defined in 49 CFR 173.403.
- Bulk liquefied chlorine gas and bulk liquefied gas cargo that is flammable and/or toxic and carried under 46 CFR 154.7.

- The following bulk liquids: (I) acetone cyanoglydrin, (II) allyl alcohol, (III) chlorosulfonic acid, (IV) crotonaldehyde, (V) ethylene chlorohydrin, (VI) ethylene dibromide, (VII) methacrylonitrile, and (VIII) oleum (fuming sulfuric acid).

CIVIL PENALTY PROCESS - The means of reporting, adjudicating, and disposing a suspected violation of Federal law where the statute or regulation provides for a civil penalty (e.g., CG-4100 violation, fisheries violation).

CLASSIFICATION SOCIETY - An organization, other than a flag State, that issues Certificates of Class and/or International Convention Certificates.

CLEAR GROUNDS - Evidence that the ship, its equipment, or its crew does not correspond substantially with the requirements of the relevant conventions or that the master or crew members are not familiar with essential shipboard procedures relating to the safety and security of the vessel.

CODE OF FEDERAL REGULATIONS (CFR) - The compilation and codification of U.S. administrative law by subject matter arranged in numerical titles. The CFR is published officially by the Federal Government in volume form.

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

CONTIGUOUS ZONE - For the purpose of determining jurisdiction over location and interpreting international law, the waters within the belt adjacent to and seaward of the territorial sea and extending to 24NM from the baseline (i.e., between 12NM and 24NM), but in no case extending within the territorial seas of another nation. For the purpose of determining the application of substantive law under the Federal Water Pollution Control Act and Title 19 USC, the waters within the belt 9NM wide that is adjacent to and seaward of the 3NM territorial sea (i.e., between 3NM and 12NM).

CONTINENTAL SHELF - The area of seabed and subsoil beyond the territorial sea, which extends up to either: 200NM from the baseline; or, subject to certain limits, the outer edge of the continental margin (the submerged prolongation of the land mass), or 100NM from the 2500 meter isobath, whichever is further seaward (but in no case beyond 350NM from the baseline).

CONTINUOUS SYNOPSIS RECORD - Record required under regulation of chapter V of SOLAS. The record will provide an on-board record of history of the ship.

CONTRACTING GOVERNMENTS AND PARTIES - Government or flag States that have legally accepted to be bound by the requirements of a convention, protocol or other instrument.

CRIMINAL OFFENSE - An offense where the statute provides for criminal penalties, such as fines or imprisonment.

DECLARATION OF SECURITY - An agreement between a vessel and a port facility that addresses security requirements that are shared between a ship and a facility and outlines both ship and facility responsibilities on their security arrangements to ensure coordination and communication is clearly established.

DEFICIENCY - A condition found not to be in compliance with the requirements of the relevant convention or regulation.

DESERTER - A crewmember that is authorized by the U.S. Citizenship and Immigration Service (USCIS) to enter, but upon entry remains illegally in the United States.

DETENTION - For law enforcement purposes, the act of keeping back, restraining or withholding a person or property for a temporary, reasonable period of time for the purpose of inspection, investigation or search when such act does not amount to an arrest or property seizure.

DOCUMENTED VESSEL - A vessel documented under U.S. law (Title 46, U.S. Code; Title 46, CFR, Subpart 67) and issued a Certificate of Documentation by the United States Coast Guard.

EXCLUSIVE ECONOMIC ZONE - For the purpose of determining jurisdiction over location and interpreting international law, the zone of waters beyond and adjacent to the territorial sea not extending beyond 200NM from the baseline. For MSFCMA purposes, the inner boundary of the EEZ is the seaward limit of U.S. states and territory jurisdiction (i.e., 3NM for most areas; 9NM for Texas, the Gulf Coast of Florida, and Puerto Rico.)

EXTENDED INITIAL SAFETY INSPECTION (EISI) - The EISI is part of the protective sweep of a vessel for the safety of the boarding team, but is more focused. An extended ISI may be conducted only when reasonable suspicion exists that there is a particular hazard that may threaten the boarding team. The scope and conduct of the EISI is guided by the suspected hazard. Further guidance on EISI can be found in Chapter 3 of the MLEM, COMDTINST M16247.1 (series).

FEDERAL REGISTER - A daily publication in which U.S. administrative agencies publish proposed regulations for public comment and final regulations.

FLAG ADMINISTRATION - All governments that have legally accepted to be bound by the requirements of a convention, protocol, or other instrument.

FLAG STATE – The nation where a given vessel is legitimately registered. The vessel claims the nationality of that nation and that nation exercises its jurisdiction and control in administrative, technical, and social matters over the vessel.

FLAG STATE AUTHORIZATION - Permission from the flag State of a vessel to board and/or take enforcement actions with respect to that vessel. Flag State authorization is obtained through a special arrangement between the U.S. and the flag State. The specific terms of the authorization determine exactly what enforcement action (e.g., boarding, search, detention, arrest, and/or seizure) the United States Coast Guard may take with respect to the foreign-flag vessel.

FOREIGN-FLAG VESSEL – Foreign-flag vessels are all seagoing vessels except U.S. vessels, vessels without nationality, and vessels assimilated to a vessel without nationality.

HEAVILY POPULATED AREA - For maritime application, cities with a population of more than 100,000 people.

HIGH INTEREST VESSEL - A commercial vessel intending to enter a U.S. port that may pose a high relative risk to the port.

HIGH SEAS - For the purpose of determining jurisdiction over location and interpreting international law, high seas are all parts of the ocean seaward of the Exclusive Economic Zone; if a coastal State has not proclaimed an Exclusive Economic Zone, the high seas begin at the seaward edge of the territorial sea. For the purpose of determining the applicability of substantive laws related to the special maritime and territorial jurisdiction of the U.S. as defined in 18 USC 7, the Great Lakes and all waters seaward of the baseline. For the purpose of determining the applicability of 33 USC 151 (High Seas demarcation lines for COLREGS) and 33 USC 2072 (Inland Navigation Rules), the waters seaward of any lines established pursuant to those statutes, including the lines described in 33 CFR Part 80.

IMO DETENTION - Intervention action taken by the port State when the condition of the ship or its crew does not comply substantially with the applicable conventions. Detentions ensure that the ship will not sail until it can proceed to sea without presenting a danger to the ship or persons on board, or without presenting an unreasonable threat or harm to the marine environment, whether or not such action will affect the normal schedule of the departure of the ship.

INSPECTION - An examination of government licensees and regulated businesses or activities for compliance with government regulations.

INITIAL SAFETY INSPECTION (ISI) - The initial safety inspection (ISI) is conducted to identify any safety hazards that may exist and ensure the seaworthiness of the vessel being boarded. There are two levels of initial safety inspection: (1) basic; and (2) extended. Further guidance on ISI can be found in Chapter 3 of the MLEM, COMDTINST M16247.1.

INTERNAL WATERS - For the U.S., the waters shoreward of the baseline, including all waters on the U.S. side of the international boundary of the Great Lakes. For any other nation, the waters shoreward of its baseline as recognized by the U.S.

INTERNATIONAL MARITIME ORGANIZATION (IMO) - Specialized agency of the United Nations concerned solely with maritime affairs. Responsible for international treaties, conventions, resolutions, and codes to improve maritime safety.

INTERNATIONAL SHIP AND PORT FACILITY SECURITY CODE (ISPS) – IMO assembly adopted document that establishes an international framework involving co-operation between Contracting Governments, Government agencies, local administrations and the shipping and port industries to detect and access security threats. The ISPS Code applies to the following types of ships engaged on international voyages: passenger ships including high-speed passenger craft, and cargo ships of 500 gross tonnage and upwards including high-speed craft.

INTERNATIONAL WATERS - The waters seaward of the outer limit of the territorial sea of any nation, but encompassing the high seas, exclusive economic zone (EEZ), and contiguous zones.

JURISDICTION - The government's right to exercise legal authority over its persons, vessels and territory. Within the context of maritime law enforcement, jurisdiction is comprised of three elements: substantive law, vessel status/flag State, and location.

KEY ASSETS (KA) - See MARITIME CRITICAL INFRASTRUCTURE/KEY ASSETS (MCI/KA).

LAW ENFORCEMENT AGENCY - An executive agency chartered and empowered to enforce laws in one of the following jurisdictions: U.S., a state (or political subdivision) of the U.S., a territory or possession (or a political subdivision) of the U.S., or the borders of a foreign nation.

MANIFEST - A collection of forms required for presentation on a vessel's arrival or departure in/from the United States. Typically these include, but are not limited to, Form I-418 (Crew List), Form I-92 (Vessel Report), Form I-94 (Arrival/Departure Record) and Form I-95 (Conditional Landing Permit).

MARINE TRANSPORTATION SYSTEM (MTS) - Consists of waterways, ports and intermodal connections, vessels, vehicles, and system users, as well as federal maritime navigation systems.

MARITIME CRITICAL INFRASTRUCTURE/KEY ASSETS (MCI/KA) - Facilities, structures, systems, assets, or services so vital to the port and its economy that their disruption, incapacity, or destruction would have a debilitating impact on defense, security, the environment, long-term economic prosperity, public health, or safety of the port (Source: 33 CFR 101.105)

MARITIME HOMELAND SECURITY (MHS) - MHS is federal law enforcement carried out by domestic law enforcement authorities, including the United States Coast Guard (USCG), and shall be conducted in accordance with settled law enforcement procedures, the Maritime Law Enforcement Manual (COMDTINST M16247.1 (series)) and other applicable law enforcement policies. Department of Defense (DoD) personnel may assist non-DoD law enforcement

authorities with MHS law enforcement missions in accordance with federal law and applicable DoD and USCG regulations and policies. The Homeland Security Act defines the following USCG missions as homeland security missions: ports, waterways and coastal security; drug interdiction; migrant interdiction; defense readiness; and other law enforcement activities. MHS does not include the physical security of Coast Guard units and property, which shall be conducted in accordance with the Physical Security and Force Protection Manual, COMDTINST M5530.1c.

NAVAL VESSEL PROTECTION ZONE (NVPZ) - As described in 33 CFR 165, Subpart G, a NVPZ is a 500-yard regulated area of water, including a 100-yard exclusion zone, surrounding large U.S. naval vessels, including MSC vessels, in effect at all times in the navigable waters of the U.S. (out to 3nm), whether the large naval vessel is underway, anchored, moored, or within a floating drydock, except when the large naval vessel is moored within a restricted area or within a Naval Defensive Sea Area.

NAVIGABLE WATERS OF THE U.S. - For the purpose of the Federal Water Pollution Control Act, those waters shoreward of 3 nautical miles (NM) from the baseline, including internal waters and all other waters subject to federal Constitutional authority. For all other purposes, those waters shoreward of 12NM from the baseline, including internal waters subject to tidal influence and those waters not subject to tidal influence that are or have been used, or susceptible of use, as highways for substantial interstate or foreign commerce, or capable of improvement at a reasonable cost to serve as highways for substantial interstate or foreign commerce. Each Coast Guard District maintains a current list of navigable waters of the U.S. within that District.

NOTICE OF ARRIVAL – The notice that vessels must provide the United States Coast Guard before entering U.S. ports. See 33 CFR part 160 for more information.

OPERATIONAL CONTROL (OPCON) - The authority to perform those functions of command over subordinate forces involving organizing and employing commands and forces, assigning tasks, designating objectives and giving authoritative direction over all aspects of law enforcement or military operations and joint training necessary to accomplish assigned missions. OPCON may be exercised at any echelon at or below the level of Area Commander, or combatant command for joint operations, and can be delegated or transferred. OPCON, in and of itself, does not include authoritative direction for logistics, administration, discipline, internal organization, or training.

PASSENGER - Any person arriving in the United States on board a vessel who is not a CREW MEMBER or a STOWAWAY.

PORT FACILITY SECURITY OFFICER - The person designated as responsible for the development, implementation, revision, and maintenance of the port facility security plan and for liaison with the ship security officers and company security officers.

PORT FACILITY SECURITY PLAN - A plan developed to ensure the application of measures designed to protect the port facility and ships, persons, cargo, cargo transport units, and ship's stores within the port facility from the risks of a security incident.

PORT STATE CONTROL - The process by which a nation exercises its domestic and/or international authority over foreign vessels when those vessels are in waters subject to its jurisdiction.

PORT STATE CONTROL OFFICER (PSCO) - A person duly authorized by the competent authority of a Party to a relevant convention to carry out port State control inspections, and responsible exclusively to that Party.

PORTS, WATERWAYS, AND COASTAL SECURITY (PWCS) - Protect the U.S. Maritime Domain and the U.S. Marine Transportation System from internal and external threats such as: destruction, loss, or injury from terrorism, sabotage, or other subversive acts. Deny their use and exploitation as a means for attacks on U.S. territory, population, and critical infrastructure. Prepare for and, in the event of attack or incident, conduct emergency response operations. When directed, as the supported or supporting commander, transition to and conduct Maritime Homeland Defense operations.

POSITIVE CONTROL MEASURES - Concurrent with or upon completion of a security boarding, armed boarding team members establish positions aboard the vessel to deter, detect, prevent, and respond to acts of terrorism and /or transportation security incidents.

RECOGNIZED ORGANIZATION - An organization that meets the relevant conditions set forth by resolution A.739(18), and has been delegated by the flag State Administration to provide the necessary statutory services and certification to ships entitled to fly its flag.

RECOGNIZED SECURITY ORGANIZATION (RSO) - An organization with the appropriate expertise in security and antiterrorism matters recognized by the Administration [or Designated Authority] and authorized to carry out assessment, verification, approval and certification activities, required by the ISPS Code. The organization meets the 12 requirements set for in Part A of the ISPS Code to perform certain port security functions such as; approval of ship security plans, or amendments thereto, on behalf of the Administration; verification and certification of compliance of ships with the requirements of chapter XI-2 and part A of the ISPS Code on behalf of the Administration; and conducting port facility security assessments.

REGULATED NAVIGATION AREA (RNA) - To regulate navigation in a specific area where hazardous conditions exist which may make routine navigation unsafe. RNAs generally impose operating conditions/restrictions on vessels to ensure safe navigation.

REGULATION - A rule or order issued by a U.S. administrative agency, normally acting pursuant to authority granted by statute.

SAFETY ZONE - Established for the protection of vessels, structures, waterways, and shore areas; established for general safety and environmental protection purposes. It may be described

by fixed limits, or it may be a zone around a vessel in motion. Safety Zones may also be established to prevent or respond to an act of terrorism against an individual, vessel or structure

SECURITY BOARDING - An examination by an armed boarding team of a vessel (including the cargo, documentation, and persons on board) designated by the Captain of the Port (COTP), arriving or departing at a U.S. port, to deter acts of terrorism and/or transportation security incidents. COTPs may order a security boarding for vessels engaged in domestic operations if intelligence or other law enforcement information warrants. Security boardings include, but are not limited to:

- (1) Verification of the information submitted in the Notice of Arrival (NOA) submission;
- (2) Ensuring that the ship and crew are operating consistent with the stated purpose of the voyage, industry norms, and Federal law and regulations;
- (3) Investigation of any intelligence and/or law enforcement information related to the vessel and crew; and
- (4) Collection of information intended to assist the COTP in deciding whether to permit the vessel to enter or leave port.

Security boardings can be broken down into three phases consisting of (1) an initial safety inspection, (2) an administrative review of security and safety elements, and (3) a general walk-through of the vessel for security and safety compliance including verification of specific elements of the ISPS Code.

SECURITY ZONE - To safeguard vessels, harbors, ports and waterfront facilities from sabotage or other subversive acts, accidents or other causes of a similar nature.

SHIP MANAGEMENT - Owner, operator/master, and/or charter of a vessel.

SHIP SECURITY ALERT SYSTEM - System required by regulation 6 of chapter XI-2 of SOLAS. When activated, the system should initiate and transmit a ship-to-shore security alert to a competent authority as designated by the flag Administration. The system will identify the ship, its location, and indication that the security of the ship has been compromised.

SHIP SECURITY OFFICER - The person on board a ship, accountable to the master, designated by the Company as responsible for the security of the ship, including implementation and maintenance of the ship security plan and for liaison with the company security officer and port facility security officers.

SHIP SECURITY PLAN - A plan developed to ensure the application of measures on board the ship designed to protect persons on board, cargo, cargo transport units, ship's stores, or the ship from the risks of a security incident.

STATELESS VESSEL - See VESSEL WITHOUT NATIONALITY.

STATUTE - A law passed by the U.S. Congress and signed by the President.

STOWAWAY - Any person who is secreted on a ship, or in cargo which is subsequently loaded on the ship, without the consent of the ship's owner, the master, or other responsible person and who is detected on board the ship after it has departed from port, or in the cargo while unloading it in the port of arrival. Also defined as an alien coming to the U.S. surreptitiously on an airplane or vessel without legal status for admission.

SUBSTANDARD SHIP - A ship whose hull, machinery, equipment, or operational safety is substantially below the standards required by the relevant convention or whose crew is not in conformance with the safe manning document.

TERRITORIAL SEA (FOREIGN) - The waters within the belt that is adjacent to the foreign nation's coast and whose breadth and baseline are recognized by the U.S.

TERRITORIAL SEA (U.S.) - The waters within the belt, 12 nautical miles (NM) wide, that are adjacent to the coast of the U.S. and seaward of the baseline, for the following purposes:

- Determining jurisdiction over location;
- Interpreting international law;
- Determining the applicability of substantive laws within Subtitle II, Title 46 USC and the Ports and Waterways Safety Act, 33 USC 1221, and any regulations issued under the authority of these statutes;
- Determining the applicability of substantive laws within Title 18, USC; and
- Determining the applicability of substantive laws related to the special maritime and territorial jurisdiction of the U.S. as defined in 18 USC 7.

For the purpose of determining the applicability of substantive U.S. domestic laws not mentioned above, the territorial sea means the waters within the belt, 3NM wide, that is adjacent to the coast of the U.S. and seaward of the baseline.

TERRITORIAL SEA BASELINE - see BASELINE.

TERRORISM - Any activity that involves an act that is dangerous to human life or potentially destructive of critical infrastructure or key resources; and is a violation of the criminal laws of the United States or of any State or other subdivision of the United States or that would be a criminal violation if committed within the jurisdiction of the United States or of any State or subdivision of the United States; and appears to be intended to intimidate or coerce a civilian population; to influence the policy of a government by intimidation or coercion; or to affect the conduct of a government by mass destruction, assassination, or kidnapping. Further definitions or terrorism can be found in Chapter 10 of the MLEM, COMDTINST M16247.1 (series).

UNITED STATES CODE (USC) - The compilation and codification of U.S. statutory law by subject matter arranged in numerical titles. The USC is published officially by the Federal Government in volume form and kept current between publishing by annual supplements.

U.S. MARITIME DOMAIN - Encompasses all U.S. ports, inland waterways, harbors, navigable waters, Great Lakes, territorial seas, contiguous zone, customs waters, coastal seas, littoral areas, the U.S. Exclusive Economic Zone (EEZ), and oceanic regions of U.S. national interest, as well as the sea lanes to the U.S., U.S. maritime approaches, and the high seas surrounding America.

U.S. VESSEL - A vessel that:

- Is documented under 46 USC 12101-12124 (Certificate of Documentation);
- Is numbered as provided by 46 USC 12301-12309 (Certificate of Number);
- Is owned in whole or part by a U.S. citizen or national and not registered in another country; or
- Was once documented under U.S. law and, without approval of the U.S. Maritime Administration, had either been sold to a non-U.S. citizen or placed under foreign registry or flag.

VERIFICATION - A visit on board a ship to check both the validity of the certificates and other documents, and the overall security compliance condition of the ship, its equipment, and its crew.

VESSEL - Includes every description of watercraft or other contrivance used, or capable of being used, as a means of transportation in water.

VESSEL ESCORT - Provision of armed vessels and/or aircraft to enforce a moving security zone or Naval Vessel Protection Zone (NVPZ), or otherwise accompany and protect against external attack; the geographic extent of the escort shall be specified by the Operational Commander.

VESSEL OF INTEREST (VOI) - A vessel identified by the National Maritime Intelligence Center (NMIC), Area Maritime Intelligence Fusion Centers, District Intelligence Office, or other agency at the regional or port level seen as posing a potential security or criminal threat.

VESSEL WITHOUT NATIONALITY - A vessel that is not registered in one single nation. They are not entitled to fly the flag of any nation and, because they are not entitled to the protection of any nation, are subject to the jurisdiction of all nations. The following, all of which are considered affirmative claims under international law, evidences nationality:

- Oral claim of nationality by the master or other person in charge of the vessel;
- Vessel documents issued by the flag State; and
- National flag or ensign flown.

A vessel without a nation is often commonly referred to as a *stateless vessel*.

VESSEL INSPECTION - A systematic process used to ensure compliance with governmental regulations (e.g., vessel safety inspection, fisheries regulatory inspection, marine safety inspection).

WEAPON OF MASS DESTRUCTION (WMD) - Any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; a disease organism; or radiation or radioactivity.

ENCLOSURE 6

FOREIGN VESSEL EXAM BOOK FOR MTSA/ISPS CODE COMPLIANCE

United States Coast Guard



**FOREIGN VESSEL
EXAM BOOK FOR MTSA/ISPS CODE COMPLIANCE
(FOR ALL FOREIGN VESSELS)**

Name of Vessel	Flag <input type="checkbox"/> No Change
IMO Number	Case Number
Date Completed	
Location	
Senior Marine Inspectors / Port State Control/ Boarding Officers	
1. _____	5. _____
2. _____	6. _____
3. _____	7. _____
4. _____	8. _____

CG-840 ISPS
MTSA/ISPS CODE
Rev. 3DEC03

Use of Foreign Vessel MTSA/ISPS Code Exam Book

Since 1994, the Port State Control (PSC) program has had a dramatic influence upon the elimination of substandard shipping. This highly successful program will now include changes that seamlessly integrate verification and enforcement of the regulations authorized by the Maritime Transportation Security Act of 2002 (MTSA) and the provisions of SOLAS Chapter XI-2 and the International Ship and Port Facility Security (ISPS) Code into the existing port State control structure and processes.

The PSC program relies on several elements to ensure vessels not in compliance with safety and security standards do not enter or pose a hazard to the United States. These elements focus on poor performance of owners, operators, charterers, flag Administrations and those recognized organizations (RO) or recognized security organizations (RSO) an Administration may authorize to act on their behalf through:

- risk-based screening of vessels;
- on board verification on potentially non-compliant vessels; and
- enforcement actions that may include, among other actions, denial of entry, detention, or ordering a vessel out of port.

Security examinations shall be done at the location specified by the COTP based on the priority established by targeting risk factors. For example, an arriving vessel that receives a high risk score could be boarded at sea, prior to port entry, for the purpose of conducting a security and safety sweep of the vessel. Vessels posing less risk may be boarded for examination at the pier or not at all. In every case, vessels selected for security boarding will be boarded in accordance with the applicable international and domestic standards. The scope of the security examination shall be as determined by the COTP and the applicable provisions of Title 33 CFR, SOLAS Chapter XI-2, and ISPS Code Parts A and B and this Exam Book shall apply. Note that for many requirements, compliance with Part A of the ISPS Code can be inferred from compliance with Part B because of the greater detail in Part B. It is important to note that every vessel only selected for a port State control safety boarding may also be subject to some measure of security examination in accordance with Part A and Part B of the ISPS Code and the checklist herein may be used to guide this abbreviated security examination.

To meet port State responsibilities, senior marine inspectors/port State control officers must verify that the vessels and their crews are in substantial compliance with international conventions and applicable U.S. laws related to security. The senior marine inspectors/port State control officers, based on their observations, must determine the depth and scope of the examination.

This exam book does not establish or change Federal or International standards. References given are only general guides. Refer to IMO publications, United States Code, the Code of Federal Regulations, NVIC's, and any locally produced guidance for specific regulatory references. This checklist is an extensive list of possible examination items related to security equipment, operations, plans and records. It is intended as a job aid to be used by Coast Guard marine inspectors during examinations of foreign-flagged vessels subject to regulations authorized by MTSA, and provisions of SOLAS Chapter XI-2 and the ISPS Code. It is not the Coast Guard's intention to inspect all the items listed in the checklist at every exam; rather the inspector should use it as a reminder of the various items that may be examined during a security examination. As always, the inspector's experience, knowledge, and judgment will determine the depth and scope of each examination.

Conducting the exam

- Complete Certificates/Equipment Data/Records information (Section A).
- Review Vessel Security Practices and Competencies (Section B).
- Expanded Examination (only if Clear Grounds are exist) (Section C)

Pre-inspection Items	Post-inspection Items
<ul style="list-style-type: none"> • Review MISLE records • Deficiency History • Critical Profile • CG Activity History 	<ul style="list-style-type: none"> • Issue letters/certificates to vessel • Issue Port State Control Report of Inspection-Form A • Issue Port State Control Report of Inspection-Form B (if needed) • MISLE activity case

Certificates / Reports (complete at each security exam and update MISLE Certificate data)

Name of Certificate	Issuing Agency	ID #	Issue Date	Expiration Date	Endorsement Date	Official Seal (Y/N)	Remarks
International Ship Security Certificate							
Interim International Ship Security Certificate (if issued)							

Continuous Synopsis Record (Review Record and Enter Most Current Data)

Flag State	Date Registered	Ship ID #	Ship Name
Port of Registry	Registered Owners	Bareboat Charterer (if appl.)	Company (1)
Issuer -ISM Doc. Of Compliance	Issuer – ISM Safety Management Cert.	Issuer – ISM Safety Management Cert.	Issuer - ISPS International Ship Security Certificate (indicate if interim)

(1) as defined in SOLAS Chapter IX

Declaration of Security (if applicable)

Facility Name	Completed?	Date	Contact Details



Until such point that clear grounds are established, examinations shall address Parts A and B of the ISPS Code and shall be done **solely through observations** that expected security procedures are in place and though verifying the on board presence and validity of required security documents and certificates. The checklist items given below are to serve merely as reminders for items to observe as far as practicable and applicable on a particular type of ship and to the type of shipboard operations being conducted.

<p>Performance of Ship Security Duties</p> <p><input type="checkbox"/> Duties of ship personnel assigned security responsibilities and of other shipboard personnel</p> <ul style="list-style-type: none"> • Ship is at prescribed security level at port (MARSEC Level _____). • General walk-through of vessel/restricted areas to observe security provisions in place • Shipboard personnel attentive to security matters indicating active efforts being taken to ensure appropriate security measures are in place <p><input type="checkbox"/> Identification of ship security officer/company security officer</p>	<p>33 CFR 104.240(a) ISPS Part A Sect. 7.1 & 12 ISPS Code Part B Sect 9.7</p>
<p>Controlling Access to the Ship (number in parentheses indicates security level)</p> <p><input type="checkbox"/> Measures to Prevent Unauthorized Access to ship</p> <ul style="list-style-type: none"> • Security personnel require personal identification and reason to board (1) • Access points identified/manned to prevent unauthorized access (1) • Unattended spaces adjoining spaces accessible to passengers/visitors secured (1) • Security personnel appear to be briefed re: threats, suspicious persons, objects or activities and need for vigilance (1) • Security personnel patrolling deck areas (2) • Access points to ship limited (2) • Waterside access to ship deterred (2) • Restricted zone established on shore side of ship (2) • Visitors receive escort (2) • Full or partial search of ship conducted (2) • Access restricted to single point (3) • Access to ship limited to security personnel (3) • Directing persons on board (3) • Suspend embarkation/debarkation or evacuate ship (3) • Suspend cargo operations (3) • Move the ship to a more secure area (3) • Preparations taken for a full or partial search of the ship (3) 	<p>33 CFR 104.265 ISPS Part A Sect. 7.1 & 9.4 ISPS Part B Sect. 9.9 – 9.17</p>
<p>Controlling Embarkation of Persons and Their Effects (number in parentheses indicates security level)</p> <p><input type="checkbox"/> Measures to prevent unauthorized weapons, dangerous substances, and devices from being brought on board</p> <ul style="list-style-type: none"> • Secure area(s) to search persons, baggage, etc. provided (1) • Checked persons/baggage segregated from unchecked persons/baggage (1) • Embarking persons segregated from disembarking passengers (1) • Ro-ros/Ferries - vehicle searches performed (1) • Unaccompanied baggage screened/searched (1) • Frequency and detail of searches (persons, effects, vehicles) increased (2) • Unaccompanied baggage 100 percent x-ray searched (2) • Unaccompanied baggage, thorough x-ray search (different angles), or refusal to accept (3) 	<p>33 CFR 104.255 ISPS Code Part A, 7.1, 9.4 ISPS Code Part B 9.14, 9.15, 9.38 – 9.41</p>
<p>Monitoring Deck Areas and Areas Surrounding Ship (number in parentheses indicates security level)</p> <p><input type="checkbox"/> Monitoring Security of the Ship</p> <ul style="list-style-type: none"> • Mix of lighting, watchkeepers, security guards, security equipment used to observe the ship in general (1) • Stepped up use of lighting, watchkeepers, security guards, security equipment (2) • Maximized use of lighting, watchkeepers, security guards, security equipment (3) 	<p>33 CFR 104.285 ISPS Part A Sect. 7.1 & 9.4 ISPS Part B Sect. 9.42 – 9.49</p>

<p>Monitoring Restricted Areas Ensuring only Authorized Persons have Access, e.g. (number in parentheses indicates security level)</p> <p><input type="checkbox"/> Restricted Areas Monitored/Measures to Prevent Unauthorized Access (examples: Bridge, Engine Room, Steering Compartment, Cargo Control Room, Pump Room, Cargo Spaces, CO2 Room, etc.)</p> <ul style="list-style-type: none"> • Surveillance Equipment in use (1) • Locked/ Secured/ Roving guard for access points (1) • Intrusion alarms devices in use (1) • New restricted areas established adjacent to access points (2) • Continuous use of surveillance equipment (2) • Added guards for access points (2) • Restricted areas established in proximity to security incidents (3) • Restricted areas searched (3) 	<p>33 CFR 104.270 ISPS Part A Sect. 7 & 9.4 ISPS Part B Sect. 9.18 – 9.24</p>
<p>Supervision of Cargo and Ship's Stores (number in parentheses indicates security level)</p> <p><input type="checkbox"/> Procedures for security of cargo & stores and for cargo & stores operations</p> <ul style="list-style-type: none"> • cargo, transport units, and cargo spaces routinely checked before operations (1) • cargo checked for match to cargo documentation (1) • vehicles routinely searched prior to loading (1) • anti-tamper seals/methods checked (1) • cargo visually/physically examined (1) • scanning equipment/dogs used (1) • stores checked for match order prior to loading (1) • stores stowed immediately (1) • cargo, transport units, and cargo spaces checked in detail before operations (2) • intensified checks that only intended cargo is loaded (2) • vehicles search intensively prior to loading (2) • anti-tamper seals/methods checked with greater frequency and detail (2) • cargo visually/physically examined with greater frequency and detail (2) • scanning equipment/dogs used with greater frequency and detail (2) • enhanced security measures coordinated with shipper/responsible party iaw an established agreement (2) • stores more extensively checked for match order prior to loading (2) • cargo loading/unloading suspended (3) • verifying the inventory of dangerous and hazardous goods and their location (3) • stores more intensively checked, suspended, or refusal to accept (3) 	<p>33 CFR 104.275, 104.280 ISPS Code Part A 7.1, 9.4 ISPS Code Part B 9.25 – 9.37</p>
<p>Security Communication is available</p> <p><input type="checkbox"/> Procedures and equipment for communicating responses to security threats and communicating with port, port State, and flag State</p> <ul style="list-style-type: none"> • Security Personnel have ready access to communications – ship to flag, ship to shore, SSO to security personnel 	<p>33 CFR 104.245 SOLAS Chap. V, Reg. 19</p>
<p>Other Items</p> <p><input type="checkbox"/> Security Certificates Valid</p> <ul style="list-style-type: none"> • International Ship Security Certificate (or Interim) • Continuous Synopsis Record On Board and Kept Up-to-Date • Declaration of Security (If applicable) <p><input type="checkbox"/> Hull Markings</p> <p><input type="checkbox"/> Security Related Records</p> <ul style="list-style-type: none"> • Records of Drills and Exercises • Records of Security Threats, Incidents, & Security Breaches • Records of Changes to Ship Security Levels • Record of Security Communications • Records protected Against Unauthorized Access 	<p>33 CFR 104.250 SOLAS Chap XI-1, Reg. 5 SOLAS Chap XI-2, Reg. 9.1.2</p> <p>SOLAS Ch. XI-1, Reg. 3</p> <p>33 CFR 104.235 SOLAS Ch. XI-1, Reg. 5 ISPS Part A Sect. 10.1 ISPS Part B Sect. 10</p>

The following list of questions is intended for use as a job aid to determine whether the vessel's security personnel and procedures are in keeping with regulations issued under MTSA and the provisions of SOLAS Chapter XI-2, and the International Ship and Port Facility Code Parts A and B. This list is by no means a complete listing of appropriate questions, but is provided as an example of appropriate questions that may be used during the expanded examination to determine that personnel are properly trained and that meaningful security procedures are in place. **Boldfaced questions may only be asked if the flag State has given permission to review the portion of the security plan related to that question.**

To the Ship Security Officer:

What do you do if there is a security breach? Or security threat?

How does the security alert system work? What happens if the security alert system is activated?

What do you do if the port is at a higher security level than the ship?

What are the vessel's restricted areas? How do you restrict access to these areas?

How often is the security equipment calibrated? Ask to see records.

How do you coordinate security activities with the port facility?

When would you limit shore to ship access to only one access point?

How often do you audit security activities? How do you audit a security activity? Ask for an example. Also ask to see records.

Who is the Company Security Officer? Do you have 24/7 contact information for this person? Ask to see information.

Do you have any active Declarations of Security? And with whom?

How often do you hold security drills, training, or exercises? When was the last time you conducted a security drill, training session, or exercise? Ask to see associated records.

How do you report security breaches or incidents? Ask to see records.

What do you do if someone tries to bring an unauthorized weapon on board the vessel? Dangerous substance? Device?

How do you prevent unauthorized persons from coming on board?

Who on board are assigned security duties?

When was the last time the SSP was reviewed? Was it updated? Ask to see record of update.

What do you do to search persons and their belongings when they come on board?

What are your procedures to search unaccompanied baggage? How do these become more rigorous if security level increases?

How do you monitor the security of the ship when underway? When pierside? At anchor?

Do you have procedures in place to bring on board additional security personnel? Please describe.

Do you have procedures in place to ensure security for cargo handling? Please describe.

How do you safeguard the Ship Security Plan?

To Crew members having security responsibilities:

Who is the Ship Security Officer?

What do you do if there is a security breach? Or security threat?

How does the security alert system work? What happens if the security alert system is activated?

What are the vessel's restricted areas? How do restrict access to these areas?

When was the last time you participated in a security drill, training session, or exercise?

How do you report security breaches or incidents?

What do you do if someone tries to bring an unauthorized weapon on board the vessel? Dangerous substance? Device?

How do you prevent unauthorized persons from coming on board?

What do you do to search persons and their belongings when they come on board?

What are your procedures to search unaccompanied baggage?

How do you monitor the security of the ship when underway? When pierside? At anchor?

To Crewmembers not having security responsibilities:

Who is the Ship Security Officer?

What do you do if there is a security breach? Or security threat?

AGENT

Vessel representative hired by the ship's owners. Ship's agent may be tasked with various jobs such as: ensuring proper vessel documentation and compliance.

CARGO SHIP

Any ship which is not a passenger ship.

CLEAR GROUNDS

Evidence (including observations) or reliable information that the ship does not correspond with the requirements of SOLAS Chapter XI-2 or Part A of the ISPS Code, taking into account the guidance of Part B of the ISPS Code.

COTP

Captain of the Port.

CSO

Company Security Officer

DECLARATION OF SECURITY

An agreement between a vessel and a port facility that addresses security requirements that are shared between a ship and a facility and outlines both ship and facility responsibilities.

IMO

International Maritime Organization. Specialized agency of the United Nations concerned solely with maritime affairs. Responsible for international treaties, conventions, resolutions and codes to improve Maritime safety.

ISM

International Safe Management

MSC

Maritime Safety Committee. One of four technical bodies of the IMO which deals with issues such as aids to navigation, vessel equipment, and construction, manning requirements handling dangerous cargoes, hydrostatic information and marine casualty information.

PASSENGER SHIP

A ship that carries more than 12 passengers.

PMS

Preventative Maintenance System

SMS

Safety Management System

SOLAS

The International Convention for the Safety of Life at Sea.

SSO

Ship Security Officer (Similar in nature to Vessel Security Officer in domestic maritime security regulations.)

SSP

Ship Security Plan (Similar in nature to Vessel Security Plan in domestic maritime security regulations.)

STCW

The International Convention on Standards of Training, Certification and Watchkeeping for Seafarers.