



COMDTPUB 16700.4  
NVIC 04-03, CH-3

APR 23 2008

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 04-03, CHANGE 3

Subj: CH-3 to GUIDANCE FOR VERIFICATION OF VESSEL SECURITY PLANS ON DOMESTIC VESSELS IN ACCORDANCE WITH THE MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATIONS AND INTERNATIONAL SHIP & PORT FACILITY SECURITY (ISPS) CODE

Ref: (a) 33 CFR Part 101  
(b) 33 CFR Part 104  
(c) International Ship & Port Facility Security (ISPS) Code

1. PURPOSE. This change to Navigation and Vessel Inspection Circular (NVIC) 04-03 provides guidance on the acceptable documentary evidence to show that an individual serving as a Vessel Security Officer (VSO) has met the qualification requirements in 33 CFR 104.215 and the training requirements in the International Ship and Port Facility Security (ISPS) Code.

2. ACTION.

- a. Vessel owners, operators, and masters should become familiar with the documentary evidence necessary to show compliance with the requirements for vessel security officers.
- b. Coast Guard Captains of the Port (COTP) and Officers in Charge, Marine Inspection (OCMI) are encouraged to bring this circular to the attention of marine interests within their zones of responsibility. This circular will be distributed by electronic means only. It is available on the HOMEPOR internet website at: <http://homeport.uscg.mil>.

DISTRIBUTION – SDL No. 141

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B		8	*		5									150	1	1	2									5
C					*								*													
D	1	2		1*	1						1*	*														
E														2	*											
F			1							1																
G																										
H																										

NON-STANDARD DISTRIBUTION: See Page 3

## NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 04-03, CHANGE 3

3. DIRECTIVES AFFECTED. Remove NVIC 04-03 Table of Contents, and insert NVIC 04-03, Change 3 Table of Contents. Also, remove NVIC 04-03, enclosure (3), and insert NVIC 04-03, Change 3, enclosure (3).
4. BACKGROUND. In December 2003, NVIC 04-03 was published establishing guidelines to assist the Coast Guard and industry in complying with the requirements for developing and submitting a VSP. The focus of the original circular was to assist in the development of a VSP. NVIC 04-03, Change 1 provided the Domestic Vessel Security Plan Verification Guide for MTS/ISPS Code and provided additional policy guidance. NVIC 04-03, Change 2 provided additional guidance regarding Ship Security Alert Systems (SSAS) and vessel audit procedures.
5. DISCUSSION.
  - a. This revised circular provides marine inspectors with clarification on the documentation that may be accepted to confirm that the qualifications of the VSO meet the requirements set out in 33 CFR 104.215 and the training requirements in the International Ship and Port Facility Security (ISPS) Code.
  - b. The VSP must contain information on the VSO qualifications, as required in 33 CFR 104.405 and the ISPS Code.
  - c. To provide guidance on the verification process of ensuring a VSO has met the qualification requirements in 33 CFR 104.215, this circular revises NVIC 04-03, enclosure (3), by amending section 9 - Vessel Security Officer (VSO), adding a new section 28 – Vessel Security Plan, and adding a new section 31 – Format of the Vessel Security Plan.
  - d. This circular also updates NVIC 04-03 Table of Contents to reflect new sections 28 and 31 of the revised enclosure (3) to NVIC 04-03.
  - e. We have also revised NVIC 04-03, Change 3, enclosure (3) by correcting non-substantive inconsistencies and/or grammatical errors.
6. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is it itself a rule. It is not intended to nor does it impose legally-binding requirements on any party. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the general public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements. You can use an alternative approach for complying with these requirements if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach (you are not required to do so), you may contact the vessel security program manager at the office of vessel activities who is responsible for implementing this guidance.
7. FORMS/REPORTS. None.

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 04-03, CHANGE 3

8. CHANGES. Changes to this Circular will be issued as necessary. Suggestions for improvements to this Circular should be submitted in writing to Commandant (CG-5431) at the address specified in the header on the first page.



BRIAN M. SALERNO  
Rear Admiral, U. S. Coast Guard  
Assistant Commandant for Marine Safety,  
Security and Stewardship

---

- Enclosures: (1) CH-3 to Navigation and Inspection Circular 04-03 Table of Contents  
(2) CH-3 to Navigation and Inspection Circular 04-03 Enclosure (3) Discussion of Specific Requirements of 33 CFR 104

Non-Standard Distribution:

- DOJ Torts Branch (Washington, DC; New York; San Francisco only) (1)
- MARAD (MRG 4700) (1)
- MSC (M-24) (1)
- NOAA Fleet Inspector (1)
- NTSB (Marine Accident Division) (1)
- World Maritime University (1)
- U.S. Merchant Marine Academy, Kings Point, NY (1)
- State University of New York Maritime College (1)
- California Maritime Academy (1)
- Maine Maritime Academy (1)
- Massachusetts Maritime Academy (1)



COMDTPUB 16000.4  
NVIC 04-03, CH-2

DEC 15 2006

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 04-03, CHANGE 2

Subj: CH-2 to GUIDANCE FOR VERIFICATION OF VESSEL SECURITY PLANS ON DOMESTIC VESSELS IN ACCORDANCE WITH THE MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATIONS AND INTERNATIONAL SHIP & PORT FACILITY SECURITY (ISPS) CODE

- Ref: (a) International Convention for the Safety of Life at Sea (SOLAS), Chapter XI-2/6  
 (b) International Ship & Port Facility Security (ISPS) Code  
 (c) International Maritime Organization MSC Circulars 622, 623, 1073, and 1190  
 (d) Title 33 Code of Federal Regulation, Part 101  
 (e) Title 33 Code of Federal Regulation, Part 104  
 (f) Maritime Law Enforcement Manual, COMDTINST M16247.1C

1. PURPOSE. This change to NVIC 04-03 provides additional guidance regarding Ship Security Alert Systems (SSAS) and vessel audit procedures. Specifically, additional guidance is provided regarding the format of ship security alert messages, the United States' response to receiving these messages, as well as recommended procedures to verify an alert message.

2. ACTION.

- a. Coast Guard Captains of the Port (COTP) and Officers in Charge, Marine Inspection (OCMI) are encouraged to bring this circular to the attention of marine interests within their zones of responsibility. This circular will be distributed by electronic means only. It is available on the World Wide Web at <http://www.uscg.mil/hq/g-m/index.htm>.

DISTRIBUTION - SDL No. 141

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B		8	*		5									150	1	1	2									5
C					*							*														
D	1	2		1*	1						1*	*														
E														2	*											
F			1								1															
G																										
H																										

## NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 04-03, CHANGE 2

- b. These guidelines may be applied to evaluate, or document vessel SSASs and vessel security audits.
3. DIRECTIVES AFFECTED. Remove NVIC 04-03 Change 1, Enclosure 5, and insert NVIC 04-03, Change 2, Enclosure 5. Also insert NVIC 04-03, Change 2 Enclosure 9.
4. BACKGROUND. The attached enclosures provide guidance on implementing the International Convention for the Safety of Life at Sea (SOLAS), Regulation XI-2/6 as it applies to U.S.-flag vessels. It is intended to provide information for U.S. Coast Guard field offices, vessel owners and operators, and others involved with ship security alerting. This change to the NVIC provides guidelines for developing systems to meet the requirements of SOLAS, Regulation XI-2/6, as well as 33 CFR 104.415.
5. DISCUSSION. This revised circular provides guidance to COTPs and OCMIs on the requirements for SSAS and how to evaluate the systems for compliance with references (c), (d), and (e). For the purpose of this guidance, the term “area” is defined as a COTP zone. The revised circular also provides audit guidance to COTPs and OCMIs.
6. INFORMATION SECURITY.
  - a. Information regarding the submission and response to SSAS and vessel auditing procedures are part of the Vessel Security Plan (VSP), which contains information that, if released to the general public, could compromise the safety or security of the vessel, 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, Area Maritime Security Committees (AMSCs), and waterway operators must follow procedures stated in 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 1520.5, will have access to information regarding SSAS. Vessel owners or operators must determine which of their employees need to know provisions of the security plans and information about the SSAS, and then restrict dissemination of these documents accordingly. To ensure that access is restricted to only authorized personnel, SSI material will not normally be disclosed under the Freedom of Information Act (FOIA).
  - 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.

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 04-03, CHANGE 2

7. **DISCLAIMER.** While the guidance contained in this document may assist the industry, the public, the Coast Guard, and other Federal and State regulators in applying statutory and regulatory requirements, the guidance is not a substitute for applicable legal requirements, nor is it itself a rule. Thus, it is not intended to, nor does it, impose legally binding requirements on any party, including the Coast Guard, other Federal agencies, the States, or the regulated community.
8. **FORMS/REPORTS.** None.



C. E. BONE

Rear Admiral, U.S. Coast Guard  
Assistant Commandant for Prevention Operations

Encl: (1) Ch-2 to Navigation and Inspection Circular 04-03 enclosure 5 Ship Security Alert Systems  
(2) Ch-2 to Navigation and Inspection Circular 04-03 enclosure 9 Vessel Auditing Guidelines

**Non-Standard Distribution:**

DOJ Torts Branch (Washington, DC; New York; San Francisco only) (1)  
MARAD (MRG 4700) (1)  
MSC (M-24) (1)  
NOAA Fleet Inspector (1)  
NTSB (Marine Accident Division) (1)  
World Maritime University (1)  
U.S. Merchant Marine Academy, Kings Point, NY (1)  
State University of New York Maritime College (1)  
California Maritime Academy (1)  
Maine Maritime Academy (1)  
Massachusetts Maritime Academy (1)



COMDTPUB 16700.4  
NVIC 04 03, CH-1

**MAY 21 2004**

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 04 03, CHANGE 1

Subj: CH-1 to GUIDANCE FOR VERIFICATION OF VESSEL SECURITY PLANS ON DOMESTIC VESSELS IN ACCORDANCE WITH THE MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATIONS AND INTERNATIONAL SHIP & PORT FACILITY SECURITY (ISPS) CODE

Ref: (a) 33 CFR Part 101  
(b) 33 CFR Part 104  
(c) International Ship & Port Facility Security (ISPS) Code

1. PURPOSE. This change to Navigation and Vessel Inspection Circular (NVIC) 04 03 is to introduce a verification guide for the implementation of the maritime security regulations mandated by the Maritime Security Act (MTSA) of 2002 and the International Ship and Port Facility Security (ISPS) Code on domestic vessels. Additional policy guidance that has been introduced since the original NVIC was published is also included as a separate enclosure.

2. ACTION.

- a. Captains of the Port (COTP) and Officers in Charge, Marine Inspection (OCMI) are encouraged to bring this circular to the attention of marine interests within their zones of responsibility. This circular will be distributed by electronic means only. It is available on the World Wide Web at <http://www.uscg.mil/hq/g-m/index.htm>.
- b. Vessel and facility owners and operators may use this circular as guidance during verification inspections and for ISSC certification inspections. These guidelines may be applied to verify compliance with the Vessel Security Plan (VSP) or Ship Security Plan (SSP) when verifying compliance and used during drills conducted to ensure crew competency.

DISTRIBUTION - SDL No. 141

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B		8	*		5									150	1	1	2									5
C					*								*													
D	1	2		1*	1						1*	*														
E														2	*											
F			1							1																
G																										
H																										

NON-STANDARD DISTRIBUTION: See Page 3

3. DIRECTIVES AFFECTED. Remove NVIC 04 03 Table of Contents, and insert NVIC 04 03, ch-1 Table of Contents. Add enclosure (7), Domestic Vessel Security Plan Verification Guide For MTSA/ISPS. Code to NVIC 04 03. Add enclosure (8), Additional Policy Guidance.

4. BACKGROUND.

- a. In December 2003, NVIC 04 03 was published establishing guidelines to assist the Coast Guard and industry in complying with the requirements for submitting a plan. The focus of the original circular was to assist in the development of a Vessels Security Plan (VSP). The circular outlined the plan review process and detailed specific plan requirements, such as for the Ship Security Alert System (SSAS) on vessels subject to SOLAS XI-2.

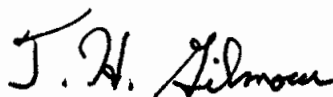
5. DISCUSSION.

- a. The intention of the guide, enclosure (7), is to provide the marine inspector with a memory jogger to guide the verification of the VSP. As outlined in the original circular, the three main objectives of the verification are to: ensure that the measures contained in the plan are in place on the vessel; to ensure that assessment accurately reflects the vulnerabilities that exist; and to ensure that the measures in the plan actually meet the needs of the vessel.
- b. The verification guide is designed to emulate the layout of a CG-840 inspection booklet. The key difference is that rather than listing particular inspection items to examine, the verification guide lists areas of the plan that must be evaluated for compliance with the three objectives listed above. This concept is a departure from the normal inspection process and is due to the performance-based nature of the MTSA regulations rather than the prescriptive format of other regulations. Nonetheless, the guide will be useful to an inspector in that it provides a roadmap for the verification process to ensure that all areas of the VSP are evaluated.
- c. The verification process for vessels is essentially the same regardless whether the vessel is subject to MTSA only, or if subject to the ISPS Code. The same is true whether the vessel has an individual VSP, or is using an Alternative Security Program (ASP). Minor differences in these verifications are noted in the guide to aid the inspector.
- d. The guide consists of a cover page, three main sections, and glossary of terms. Section (A) is required only if the is subject to ISPS. The checklist style portion of the guide in section (B) should be completed for all vessels. An explanation of each item to be verified and examples of acceptable means of verification are contained in section (C). The glossary is intended to help clarify words and terms that are unique to MTSA or ISPS Code and used throughout the guide.
- e. It is envisioned that an inspector will use the guide by completing it as each section of the VSP is verified in the presence of the Vessel Security Officer (VSO). Section (B) should be used to direct the course of the verification and ensure that all areas of the VSP are covered.



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 1520.5, 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.
7. **DISCLAIMER.** While the guidance contained in this document may assist the industry, the public, the Coast Guard, and other Federal and State regulators in applying statutory and regulatory requirements, the guidance is not a substitute for applicable legal requirements, nor is it itself a rule. Thus, it is not intended to nor does it impose legally binding requirements on any party, including the Coast Guard, other Federal agencies, the States, or the regulated community.
8. **FORMS/REPORTS.** None.



THOMAS H. GILMOUR

Rear Admiral, U.S. Coast Guard

Assistant Commandant for Marine Safety, Security  
And Environmental Protection

Encl: (7) Domestic Vessel Security Plan Verification Guide For MTSA/ISPS Code  
(8) Additional Policy Guidance

Non-Standard Distribution:

B:c CCGD13, CCGD8, CCGD7, CCGD9, CCGD5, CCGD1, CCGD11, CCGD14, CCGD14, CCGD17,  
MLCLANT, MLCPAC (2)



## NAVIGATION AND INSPECTION CIRCULAR NO. 04-03

- b. Vessel and facility owners and operators may use this circular as guidance during verification inspections and for International Ship Security Certificate (ISSC) certification inspections. These guidelines may be applied to verify compliance with the Vessel Security Plan (VSP) or Ship Security Plan (SSP) when verifying compliance and used during drills conducted to ensure crew competency.

### 3. DIRECTIVES AFFECTED. None.

### 4. BACKGROUND.

- a. The ISPS Code was developed to establish a set of international security-oriented regulations relating to vessel and port facilities. The ISPS Code facilitates cooperation among facility operators, vessel crew, vessel owners and operators, classification societies, flag States, and port States. The ISPS Code is separated into two parts: mandatory requirements in Part A and recommended guidelines in Part B. Each vessel must fully comply with all requirements outlined in Part A, while Part B offers guidance for various methods of compliance. The guidelines in Part B must be taken into consideration, but should not be considered as requirements when verifying compliance with the ISPS Code. Flag States must ensure that each vessel to which the ISPS Code applies is in compliance by conducting an on board verification inspection. The inspection entails reviewing the vessel and crew's compliance with an approved Ship Security Plan (SSP). An ISSC is issued if the vessel is found to have no deficiencies. The international standard requires a vessel and crew to be in full compliance with the ISPS Code before an interim ISSC or ISSC can be issued. To this end, inspectors must be well versed in the ISPS requirements to ensure that all measures are enforced. Regardless of when the voyage began, any SOLAS vessel (i.e., meets the service and/or tonnage criteria) that is operating in the waters of a foreign country will be considered to be on an international voyage, that was begun in a port in the United States, and therefore is subject to the ISPS Code.
- b. MTSA authorized domestic security-oriented regulations similar to the ISPS Code. Like ISPS, regulations issued under MTSA created cooperation between facility and vessel owners and operators, security personnel, crew, and the U.S. Coast Guard (USCG). The USCG is responsible for verifying that each affected vessel complies with the regulations authorized by MTSA. Vessels that are not specifically regulated under 33 CFR 104, Vessel Security, must comply with 33 CFR 103, Area Maritime Security, which is addressed in separate guidance. The regulations also closely mirror the requirement found in the ISPS Code. Compliance with the maritime security regulation suite satisfies the requirements for ISPS as well, with the exception of the requirement for the Ship Security Alert System information.
- c. Regulations issued under MTSA require the owner of each vessel covered by regulation to comply with an approved Vessel Security Plan (VSP). (SOLAS vessels must comply with a similar plan called a Ship Security Plan (SSP).) The requirements for facilities (33 CFR 105) and Outer Continental Shelf facilities (33 CFR 106) similarly require compliance with an approved security plan. The owner of a vessel not on an international voyage may chose to comply with an approved Alternative Security Program (ASP). In verifying compliance with this plan, the inspector has three tasks: ensure that the vessel or facility complies with the

approved plan, ensure that the plan and assessment adequately addresses the security vulnerabilities, and verify that the measures accomplish the intended function.

- d. Each vessel is expected to fully comply with the regulations issued under MTSA. However, due to the variety of vessel types to which these requirements apply, the method that is used in the security plan to reach compliance may vary. It is important to recognize that a deep draft vessel with a large crew, a small passenger vessel, and an uninspected towing vessel will each have unique security concerns and response capabilities. The successful performance of the VSP is the standard that must be achieved on any given verification inspection.

5. DISCUSSION.

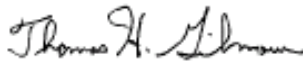
- a. This circular is designed to guide an inspector through the security plan verification process. Enclosure (1) outlines (in checklist form) the process to follow when preparing and submitting a VSP for Coast Guard approval.
- b. The general principles that an inspector may follow when conducting the VSP verification are contained in enclosure (2). This information covers broad policy issues that lay the foundation behind this program.
- c. Implementation guidance is contained in enclosure (3), and may be used if clarification is needed when completing the verification. Each heading is addressed in general terms. Where needed, additional comments are provided in italics to address specific verification issues.
- d. Background information, largely from the preamble discussion in the MTSA final rule, is contained in enclosure (4). While this information is helpful in discerning the intent of a 33 CFR 104, reviewers should realize it only addresses topics that were provided as questions or comments to the rulemaking docket. Nevertheless, the information is useful.
- e. Vessels that are subject to SOLAS XI-2 must include certain information regarding a Ship Security Alert System (SSAS) in the security plan. The information contained in enclosure (5), provides guidance on SSAS installations and technical specifications.
- f. Information regarding Alternative Security Programs (ASP) is contained in enclosure (6).

6. 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.

NAVIGATION AND INSPECTION CIRCULAR NO. 04-03

- 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 owners or operators must determine which of their employees need to know which provisions of the security plans and assessments, and 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.
7. **DISCLAIMER.** While the guidance contained in this document may assist the industry, the public, the Coast Guard, and other Federal and State regulators in applying statutory and regulatory requirements, the guidance is not a substitute for applicable legal requirements, nor is it itself a rule. Thus, it is not intended to nor does it impose legally binding requirements on any party, including the Coast Guard, other Federal agencies, the States, or the regulated community.
8. **CHANGES.** This NVIC will be posted on the web at <http://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 ALCOAST, and posted on the website for the benefit of industry pending their inclusion in to the next change to this circular. Suggestions for improvement t of this circular should be submitted in writing to Commandant (G-MOC).



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

- Encl: (1) Plan Review Guidance  
(2) 33 CFR 104: General Policy Discussion  
(3) Discussion of Specific Requirements of 33 CFR 104  
(4) Excerpts from the Preamble of 33 CFR 104  
(5) Ship Security Alert Systems  
(6) Alternative Security Programs

**Table of Contents**  
**Guidance for Verification of Vessel Security Plans on Domestic Vessels**  
**in Accordance with the Regulations Mandated by the**  
**Maritime Transportation Security Act (MTSA) of 2002 and**  
**International Ship and Port Facility Security (ISPS) Code**

**Enclosure (1) Plan Review Guidance**

Overview.....	1
Vessel Security Plan Review .....	2
How Vessel Security Plans Will Be Triage/Prioritized for Review .....	3
Alternatives to Facilitate VSP Review by MSC.....	3
Option to Submit One VSP for Multiple Similar Type Vessels .....	4
Vessels Operating under an Approved Alternative Security Program (ASP) .....	5
Submission of Plans for Foreign Vessels Subject to SOLAS.....	3

**Enclosure (2) 33 CFR 104: General Policy Discussion**

1. Overview.....	2
2. Verification Process .....	3
3. Verification Cycle.....	4
4. Verification Personnel .....	5
5. Deficiencies.....	5
6. Documentation.....	6
7. Appeals .....	7
8. International Voyages .....	7
Uninspected Towing Vessel (UTV) Examination Report .....	8

**Enclosure (3) Discussion of Specific Requirements of 33 CFR 104**

1. Instructions for Using the Guide.....	2
2. Compliance Documentation.....	2
3. Non-compliance.....	4
4. Waivers .....	4
5. Equivalents.....	5
6. Alternative Security Programs.....	5
7. Maritime Security (MARSEC) Directive .....	6
8. Company Security Officer (CSO).....	7
9. Vessel Security Officer (VSO) .....	8
10. Company and Vessel Personnel with Security Duties.....	8
11. Security Training for all Other Vessel Personnel .....	9
12. Drill and Exercise Requirements .....	9
13. Vessel Record Keeping Requirements.....	10
14. Maritime Security (MARSEC) Level Coordination and Implementation.....	10
15. Communications .....	11
16. Declaration of Security .....	11
17. Security Systems and Equipment Maintenance.....	12

18. Security Measures for Access Control.....	12
19. Security Measures for Restricted Areas.....	12
20. Security Measures for Handling Cargo.....	13
21. Security Measures for Delivery of Vessel Stores and Bunkers .....	13
22. Security Measures for Monitoring.....	14
23. Security Incident Procedures .....	14
24. Additional Requirements – Passenger vessels and Ferries.....	15
25. Additional Requirements – Cruise Ships.....	15
26. Additional Requirements – Vessels on International Voyages.....	16
27. Assessment.....	16
28. Vessel Security Plan.....	16
29. Amend and Audit.....	17
30. Ship Security Alert System (ISPS) Only .....	18
31. Format of the Vessel Security Plan (VSP).....	18

**Enclosure (4) Excerpts of the Preamble of 33 CFR 104**

1. Introduction.....	2
2. Index .....	14

**Enclosure (5) Ship Security Alert Systems**

1. Introduction.....	2
2. Definitions.....	3
3. Compliance Dates .....	4
4. Voluntary Compliance .....	4
5. Competent Authority .....	4
6. Submission of System Details for Appraisal .....	5
7. Installation of SSAS aboard SOLAS Vessels.....	6
8. System Requirements.....	6
9. Equipment Registration .....	8
10. Ship Security Alerts Messages.....	8
11. Ship Security Alert Follow Up Reports .....	7
12. Inadvertent Ship Security Alerts.....	8
13. Communications Service Providers.....	8
14. SSAS Inspection and Testing.....	9

**Enclosure (6) Guidance for Submission of Alternative Security Program (ASP), Waivers and Equivalencies**

1. Introduction.....	2
2. General Guidance.....	2
3. ASP Application Requirements .....	3
4. Action Upon Receipt of an ASP Submission .....	3
5. ASP Compliance.....	5
6. Equivalency and Waiver Application Requirements.....	5
7. Action Upon Receipt of a Waiver or Equivalency Request .....	6

**Enclosure (7) Domestic Vessel Security Plan Verification Guide For MTSA/ISPS Code**

1. Introduction.....4  
2. Section A: Certificates/Equipment Data/ Records Information.....5  
3. Section B: U.S. Flag Vessel MTSA/ISPS Code Exam Booklet .....6  
4. Section C: Additional Information..... 11  
5. Glossary of Terms/Acronyms ..... 18

**Enclosure (8) Additional Policy Guidance**

1. Introduction.....2  
2. Plan Submission.....2  
3. Plan Review .....2  
4. Certificates and Verification Examinations for U.S. Flagged Vessels Subject to SOLAS Chapter XI-2 And ISPS.....3  
5. Compliance Documentation for U.S. Flagged Vessels Operating Domestically .....4  
6. Enforcement Philosophy .....5  
7. Enforcement Cycle and Control Actions for U.S. Flagged Vessels that Operate Domestically .....7  
8. Suspending Operations .....9  
9. Intermittent Operations .....9  
10. Declaration of Security (DoS) Applicability and Interfacing with Non-Compliant Foreign Ports .....10  
11. Statements of Voluntary Compliance (SOVC).....13  
12. Continuous Synopsis Record (CSR).....13  
13. Ship Identification Number (SIN) .....14  
14. Checking Identification and Performing Passenger, Baggage, Vehicle Screening ..... 14

**Enclosure (9) Guidance for Conducting Security Audits**

1. Vessel Security Audits.....2  
2. Sample Audit Report Form.....3



**ENCLOSURE 1**  
**PLAN REVIEW GUIDANCE**

## 1. Overview

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

## 2. Vessel Security Plan Review

- A. The final rule on vessel security requires the review and approval of approximately 10,600 Vessel Security Plans (VSP) for U.S. vessels. This estimate does not include potential review of security plans for non-SOLAS foreign vessels calling on U.S. ports. Vessel owners and operators must submit their VSP to the Marine Safety Center (MSC) before 31 December 2003. The address for the MSC is:

Marine Safety Center  
400 Seventh Street, SW  
Room 6302  
Washington, DC 20590  
Voice: (202) 366-6480  
Fax: (202) 366-3877

- B. Submitters have the option of submitting paper or electronic copies (on Floppy or CD-ROM) of their VSP to MSC. The submittal and review status will be tracked in the Marine Information for Safety and Law Enforcement (MISLE) database. The status of a VSP review will be available to submitters using the Coast Guard Marine Information Exchange (CGMIX) (<http://cgmix.uscg.mil/psix/psix2/>) system.
- C. To ensure that each VSP is processed in the most efficient manner, a three-stage process will be used, which is illustrated in figure (1-1). This process will allow the Coast Guard to quickly return any plan for revision that is deficient, without the need to conduct a full plan review each time it is submitted. The first review stage is to ensure completeness, and that the basic parts required for a VSP are included in accordance with 33 CFR 104.405. The second stage will consist of a comprehensive review for compliance with vessel security regulations issued under MTSA, as well as an evaluation of any items identified as deficient in the first stage. The third stage will ensure quality and consistency of the review process.

**3. How Vessel Security Plans Will Be Triage/Prioritized For Review**

Any VSP obviously lacking significant critical information will be returned immediately. The MSC will attempt to review each complete VSP on a first submitted, first reviewed basis; however, vessels subject to SOLAS/ISPS Code (vessels in international trade) will be given priority. The initial goal is to review all substantially complete plans within 60 business days of receipt, and to return incomplete plans to the submitter for revision within 30 business days of receipt. In the event that plans reviewed as satisfactory in their completeness cannot be comprehensively reviewed by the compliance date (1 July 2004), the final rules mandated by MTSA allows the MSC to issue an interim approval letter to the vessel owner. Vessels subject to the ISPS Code must be in compliance with an approved plan to receive a certificate, which is why these vessels will be given priority for review.

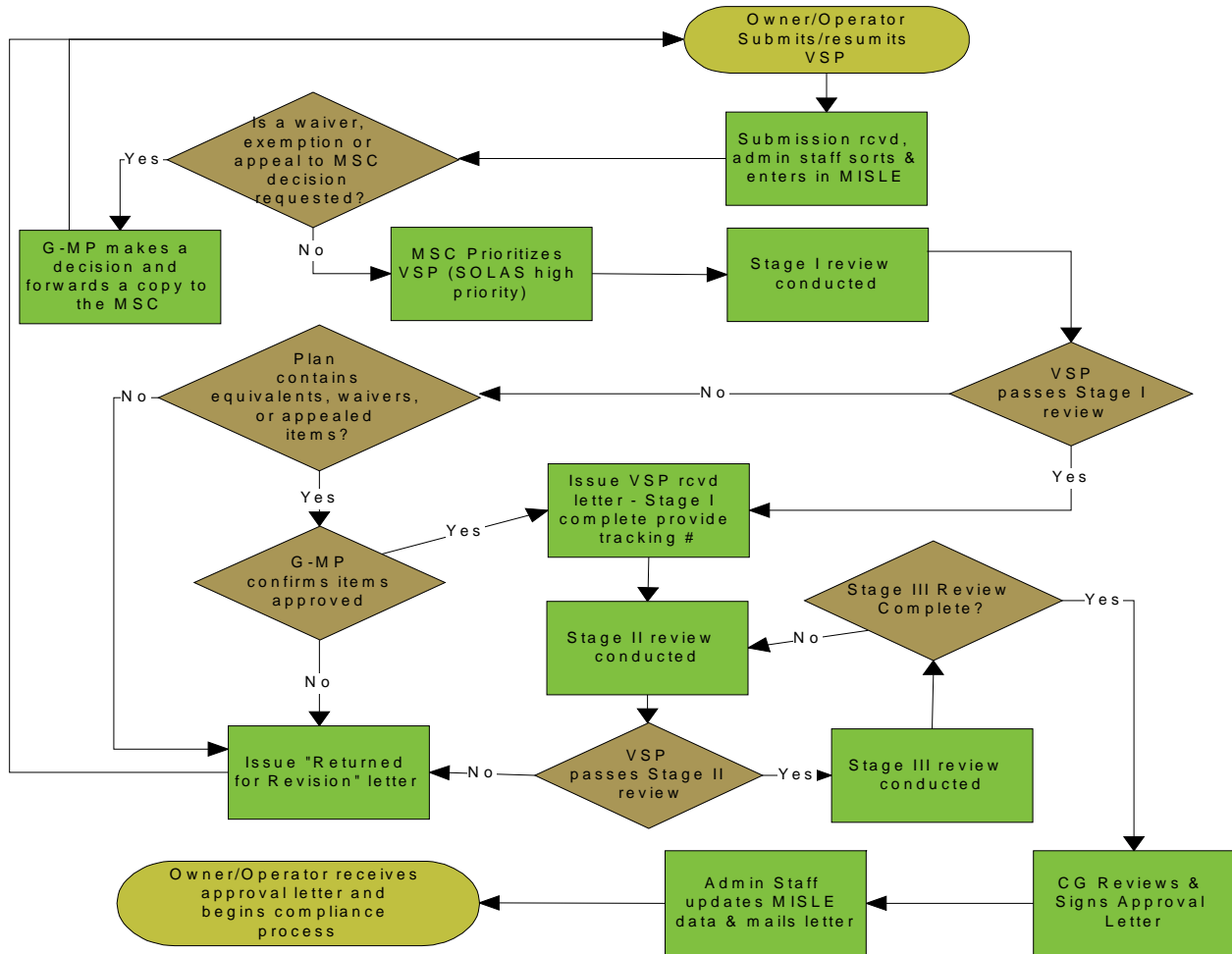


Figure 1-1

**4. Alternatives to Facilitate VSP Review by the MSC**

In order to facilitate/expedite a VSP plan review for owners/operators with more than one vessel, one VSP may be submitted to cover multiple vessels instead of a separate VSP for each vessel in accordance with 33 CFR Part 104.

**5. Option to Submit One VSP for Multiple Similar Type Vessels**

In accordance with 33 CFR 104.400(a)(6), an owner/operator may submit a VSP that covers more than one vessel to the extent that these vessels share similarities in physical characteristics and operations. Each “multiple-vessel” VSP must contain the vessel particulars for each vessel that the VSP applies to in an appendix. The name and official number must also be provided for each vessel listed in the appendix. The key to the submission of one VSP for multiple vessels is that each vessel listed in the appendix of the VSP must share similar attributes of physical design, service, and operation. A Vessel Security Assessment (VSA) Report needs to address the vessels listed.

**6. Vessels Operating under an Approved Alternative Security Program (ASP)**

If intending to operate under an approved ASP, a letter signed by the vessel owner or operator is required to be submitted to the MSC in accordance with 33 CFR 104.115(b)(2). This letter should specify the vessel name, official number, vessel type (e.g., tug, barge, casino, ferry, tank vessel, etc.) and the specific (G-MP) approved ASP being applied. The letter should also state that the ASP is being applied in its entirety. As a reminder, the ASP is not authorized for vessels on an international voyage. Detailed guidance regarding ASPs is contained in enclosure (6).

**7. Submission Of Plans for Foreign Vessels Subject to SOLAS**

In accordance with 33 CFR 104.115, owners or operators of foreign vessels subject to SOLAS and the ISPS Code must have security plans approved and verified by their Flag Administration or a Recognized Security Organization (RSO) on behalf of the Flag Administration, and must carry on board a valid International Ship Security Certificate (ISSC) issued in accordance with section 19 of Part A of the ISPS Code. This includes ensuring the vessel meets the requirements of SOLAS Chapter XI-2 and the ISPS Code, Part A, having taken into account the relevant provisions of Part B. However, these vessels **are not required to submit Vessel Security Plans to the U.S. Coast Guard for approval.** Furthermore, owners or operators of these vessels **should not** prepare or submit for approval a U.S. Annex to the VSP.

**8. Job Aid for Establishing Protective Measures**

The job aid contained in table (1-1) is a DRAFT of what will be used by the MSC to measure compliance with the requirements for an approved VSP. Industry may find this information helpful when developing a VSP.

**Table 1-1: Job aid for measuring compliance**

	COMPLIANCE	
	YES (X)	NO (X)
<b>104.205 Master</b>		
a) Authority of Master to make decision to maintain the safety and security of the vessel.		
b) If there is a conflict between safety and security, Master can take action to best maintain the safety of the vessel. In such cases:		
1) The Master must notify the Captain of the Port (COTP).		
2) Security measures must be commensurate with the prevailing MARSEC Level.		
3) Owner/operator must ensure that conflicts are resolved to the satisfaction of the COTP or the Commandant (G-MP) for vessels on international voyages, and that recurrence is minimized.		
<b>104.210 Company Security Officer (CSO)</b>		
a) <b>General.</b>		
1) Owner/Operator must designate a CSO in writing.		
2) If more than one CSO, each CSO must have designated ships for which responsible.		
3) CSO may perform other duties including those of the VSO, provided he/she is able to perform required of CSO.		
4) The CSO may delegate duties, but the CSO remains responsible for the performance of those duties.		
b) <b>Qualifications.</b>		
CSO must have general knowledge through training or equivalent experience in the following:		
1) Security administration and organization of company's vessels;		
2) Vessel, facility and port operations relevant to that industry;		
3) Vessel and facility security measures, requirements at the different MARSEC Levels;		
4) Emergency preparedness and response and contingency planning;		
5) Security equipment and systems;		
6) Methods of conducting audits, and techniques for inspecting, controlling, and monitoring techniques; <b>and</b>		
7) Techniques for security training and education, including security measures/procedures.		
c) <b>Responsibilities</b>		
In addition to duties specified elsewhere, the CSO for each vessel must:		
1) Keep vessel appraised of potential threats;		
2) Ensure a Vessel Security Assessment is carried out;		
3) Ensure a Vessel Security Plan (VSP) is developed, approved and maintained;		
4) Ensure the VSP is modified when necessary;		
5) Ensure the vessel's security activities are audited;		
6) Arrange for Coast Guard inspections under 46 CFR Part 2;		
7) Ensure timely correction of problems identified by audits;		
8) Enhance awareness and vigilance within the ship-owners organization;		
9) Ensure personnel receive adequate security training;		

10) Ensure communication/cooperation with vessel, facility, and/or port;		
11) Ensure consistency between security requirements and safety requirements;		
12) Ensure that vessel specific information is included when several similar types vessel plans are submitted;		
13) Ensure compliance with Alternative Security Plan (ASP) or equivalent, if appropriate, <b>and</b>		
14) Ensure security measures give consideration and/or convenience to vessels crew.		
<b>104.215 Vessel Security Officer (VSO)</b>		
<b>a) General</b>		
1) A VSO may perform other duties within an Owner/Operator's organization, provided he/she is able.		
2) For manned vessels the VSO must be the Master or a member of the crew.		
3) For unmanned vessels the VSO must be a company employee and may serve as VSO for more than one unmanned vessel. If serving as VSO for more than one unmanned vessel, list of vessels for which responsible must be in the VSP.		
4) The VSO of any unmanned barge and the VSO of any interfacing towing vessel must coordinate/implement security measures for interfacing period.		
5) VSP may assign security duties to other vessel personnel; however VSO responsible.		
<b>b) Qualifications</b>		
VSO must have knowledge through training or equivalent job experience in the following:		
1) Those items listed in 104.210 (b)(1) and (b)(2) of this part;		
2) Vessel layout;		
3) The VSP and related procedures including scenario-based response training;		
4) Crowd management and control techniques;		
5) Operation of security equipment and systems; <b>and</b>		
6) Testing, calibration, and maintenance of security equipment and systems.		
<b>c) Responsibilities</b>		
In addition to the duties and responsibilities mentioned elsewhere, the VSO must perform the following:		
1) Regularly inspect the vessel to ensure security measures are maintained;		
2) Ensure maintenance and supervision of implementation of the VSP and amendments;		
3) Ensure coordination of handling cargo, vessel stores and bunkers in compliance with rule;		
4) Propose modifications to the VSP to the CSO;		
5) Ensure any problems during audits/inspections are reported to the CSO and implement;		
6) Ensure security awareness and vigilance onboard the vessel;		
7) Ensure adequate training for the vessel personnel;		
8) Ensure the reporting and recording of all security incidents;		
9) Ensure the coordination/implementation of the VSP with the CSO and Facility Security Officer (FSO) when applicable;		
10) Ensure security equipment is properly operated, tested, calibrated, and maintained; <b>and</b>		
11) Ensure consistency between security requirements and proper treatment of crew.		
<b>104.220 Company or Vessel Personnel with Security Duties</b>		
These persons must have knowledge, through training or equivalent experience in the following areas:		
a) Knowledge of current security threats and patterns;		

b) Recognition and detection of dangerous substances and devices;		
c) Recognition of characteristics/behavioral patterns of those likely to threaten security;		
d) Techniques used to circumvent security measures;		
e) Crowd management and control techniques;		
f) Security-related communications;		
g) Knowledge of emergency procedures and contingency plans;		
h) Operation of security equipment and systems;		
i) Testing, calibration and maintenance of security systems while at sea;		
j) Inspection, control and monitoring techniques;		
k) Relevant provisions of the security plan;		
l) Methods of physical screening of persons/personal effects/baggage/cargo/vessels stores; <b>and</b>		
m) The meaning and consequential requirements of different MARSEC Levels.		
<b>104.225 Security Training for all Other Vessel Personnel.</b>		
All other personnel including contractors must have knowledge of, through training, or equivalent job experience in the following, as appropriate:		
a) Relevant provisions of the VSP;		
b) The consequential requirements of the different MARSEC Levels;		
c) Recognition and detection of dangerous substances and devices;		
d) Recognition and characteristics/behavioral patterns of those likely to threaten security; <b>and</b>		
e) Techniques used to circumvent security measures.		
<b>104.230 Drill and Exercise Requirements.</b>		
<b>a) General.</b>		
1) Drills and exercises test the proficiency of the crew at different MARSEC Levels and implement VSP. They must enable VSO to identify any related security deficiencies needed to be addressed.		
2) A drill or exercise may be satisfied with implementation of security measures required by VSP as result of increase in MARSEC Level, provided vessel reports attainment to the COTP.		
<b>b) Drills.</b>		
1) VSO must ensure that at least one security drill is conducted at least once every 3 months.		
2) Drills must test individual elements of the VSP including response to threats/incidents.		
3) If the vessel is at a facility which is scheduled for a drill, the vessel may participate in same drill.		
4) Drill must be conducted within one week from when crew w/o drill experience on that vessel exceeds 25%.		
<b>c) Exercises.</b>		
1) Exercises must be conducted each calendar year with no more than 18 months between exercises.		
2) Exercises may be:		
i) Full scale or live;		
ii) Tabletop simulation or seminar;		
iii) Combined with other appropriate exercises; <b>or</b>		
iv) A combination of elements in paragraphs (c) (2) (i) through (iii) of this section.		

3) Exercises may be vessel specific or cooperative to incorporate facility/vessel/port exercises.		
4) Each exercise must test communication/notification/coordination/resources & response.		
5) Exercises are a full test of security program to include company/crew/facility/government resources.		
<b>104.235 Vessel Recordkeeping Requirements.</b>		
a) The VSO must keep records of activities in paragraph (b) of this section for at least 2 years.		
b) Records required by this section may be kept in electronic format and must be protected. The following records must be kept:		
1) Training;		
2) Drills and exercises;		
3) Incidents and breaches of security;		
4) Changes in MARSEC Levels;		
5) Maintenance, calibration and testing of security equipment;		
6) Security threats;		
7) Declaration(s) of security; <b>and</b>		
8) Annual audit of the VSP;		
c) Any records required by this part must be protected from unauthorized access or disclosure		
<b>104.240 MARSEC Level Coordination and Implementation</b>		
a) Owner/Operator must ensure prior entering port or visiting an OCS facility, all measures taken as in VSP for compliance with MARSEC Level in effect in that port/facility.		
b) When notified of increase in MARSEC Level, vessel Owner/Operator must ensure the following:		
1) If higher MARSEC Level set for port which vessel is in or about to enter, vessel complies without undue delay with all measures specified in VSP for compliance with that higher MARSEC Level;		
2) The COTP is notified as required by 101.300 (c) when compliance with higher MARSEC Level is implemented;		
3) For vessels in port that compliance with higher level has taken place within 12 hours of notification, <b>and</b>		
4) If higher MARSEC Level set for OCS facility to be visited, the vessel complies without delay, with all measures specified in the VSP for compliance with that higher MARSEC Level.		
c) For <b>MARSEC Levels 2 and 3</b> , VSO must brief crew of threats/reporting procedures, and stress need for high vigilance.		
d) Owner/Operator whose vessel is not in compliance with requirements in this section must inform COTP to obtain approval prior to entering any port, to interfacing with another vessel or facility, or to continuing operations.		
e) For <b>MARSEC Level 3</b> , Owner/Operator may be required to implement additional measures that may include the following:		
1) Arrangements to ensure that vessel can be towed or moved if deemed necessary by USCG;		
2) Use of waterborne security patrol;		
3) Use of armed security personnel to control access to vessel and to deter a security		



incident; or		
4) Screening the vessel for presence of dangerous substances and devices underwater or other threats.		
<b>104.245 Communications</b>		
a) The VSO must have a means to effectively notify crew of changes in security conditions onboard vessel.		
b) Communication systems and procedures must allow effective and continuous communication between vessel security personnel, interfacing facilities/vessels and national or local authorities with security responsibilities.		
c) Communication systems and procedures must enable vessel personnel to notify shore side authorities or other vessels of a security threat or incident onboard in a timely manner.		
<b>104.250 Procedures for Interfacing with Facilities and Other Vessels.</b>		
a) Vessel Owner/Operator must ensure interface measures with other vessels/facilities at all MARSEC Levels.		
b) For each U.S. flag vessel calling foreign ports/facilities, owner/operator must ensure procedures for interfacing w/same are established.		
<b>104.255 Declaration of Security (DOS)</b>		
a) Each vessel must have procedures for requesting DoS and handling DoS requests from facility or other vessel.		
b) At <b>MARSEC Level 1</b> cruise ship or manned vessel with certain dangerous cargo (CDC) in bulk, Master/VSO must complete DoS with VSO or Facility Security Officer (FSO) of interfacing vessel/facility.		
1) For vessel-to-facility interface, prior cargo transfer/passengers FSO or Master, VSO or designee must sign DoS.		
2) For vessel-to-vessel interface, prior cargo transfer/passengers respective Masters/FSO/VSO or designee must sign DoS.		
c) At <b>MARSEC Levels 2 and 3</b> , respective Master/VSO/designee for manned vessel before vessel-to-vessel interface and prior to passenger/cargo transfer must sign DoS.		
d) At <b>MARSEC Levels 2 and 3</b> , respective Master/VSO/designee for manned vessel before vessel-to-facility interface and prior to passenger/cargo transfer must sign DoS.		
e) At <b>MARSEC Levels 1 and 2</b> , VSO of vessel that frequently calls same facility, may implement continuous DoS provided:		
1) The DoS is valid for the specific MARSEC Level;		
2) The effective period at MARSEC Level 1 does not exceed 90 days; <b>and</b>		
3) The effective period at MARSEC Level 2 does not exceed 30 days.		
f) When MARSEC Level increases beyond level in DoS, continuing DoS is void and a new one required.		
g) COTP may require at anytime at any MARSEC Level any manned vessel to implement DoS with VSO/FSO prior to vessel-to-vessel activity or vessel-to-facility interface when deemed necessary.		
<b>104.260 Security Systems and Equipment Maintenance.</b>		
a) Security systems/equipment to be in good order and tested/calibrated/maintained according to manufacturer's recommendations.		

b) Results of tests as per paragraph (a) to be recorded in accord with 104.235. Deficiencies to be promptly corrected.		
c) VSP must include procedures for identifying and responding to security equipment failures/malfunctions.		
<b>104.265 Security Measures for Access Control.</b>		
a) <b>General</b> - Vessel Owner/Operator must ensure implementation of security measures to:		
1) Deter unauthorized introduction of dangerous substances or devices;		
2) Secure dangerous substances that are authorized by the owner to be onboard; <b>and</b>		
3) Control access to the vessel;		
b) The vessel owner or operator must ensure the following are specified:		
1) Access locations where restrictions are applied for each MARSEC Level. Means of access include but are not limited to the following:		
i) Access ladders;		
ii) Access gangways;		
iii) Access ramps;		
iv) Access doors, side scuttles, windows and ports;		
v) Mooring lines and anchor chains; <b>and</b>		
vi) Cranes and hoisting gear.		
2) The types of restriction to be applied and the means of enforcing them; <b>and</b>		
3) The means of identification required to allow persons to access the vessel and remain onboard without challenge.		
c) Owner/Operator to ensure ID system to check crew/others seeking access to the vessel that:		
1) Allows ID of authorized and unauthorized persons at any MARSEC Level;		
2) Is Coordinated with ID system at facilities used by the vessel when practical;		
3) Is updated regularly;		
4) Uses disciplinary measures to discourage abuse;		
5) Allows temporary or continuing access for crew and visitors through use of badge or other system; <b>and</b>		
6) Allows certain long-term vendor representatives to be treated more as employees than as visitors.		
d) The Owner/Operator must include in VSP frequency of application of security measures for access control.		
e) <b>MARSEC Level 1</b> - Owner/Operator must ensure that the security measures in this paragraph are implemented to:		
1) Screen persons, baggage/personal effects/vehicles for dangerous substances/devices at rate indicated in the VSP, except for gov't-owned vehicles on official business with proper credentials for entry.		
2) Conspicuously post signs describing security measures in effect and clearly stating:		
i) Boarding the vessel is deemed valid consent to screening or inspections; <b>and</b>		
ii) Failure to consent to screening/inspection will result in denial or revocation of authorization to board.		
3) Check ID of any person seeking to board the vessel, including vendors, passengers, crew, visitors, etc. This check includes confirming the reason for boarding by examining at least one of the following:		
i) Joining instructions;		
ii) Passenger tickets;		

Enclosure (1) of NAVIGATION VESSEL INSPECTION CIRCULAR No. 04 03

iii) Boarding passes;		
iv) Work orders, pilot orders, or survey of orders;		
v) Government identification; <b>or</b>		
vi) Visitor badges issued in accordance with an ID system required in paragraph (c) of this section;		
4) Deny or revoke a persons authorization to be onboard if unable or unwilling to establish ID. Any such incident must be reported in compliance with this part;		
5) Deny unauthorized access to the vessel;		
6) Identify access that must be secured or attended to deter unauthorized access;		
7) Lock or prevent access to unattended spaces that adjoin areas to which passengers/visitors have access;		
8) Provide a designated area onboard for conducting inspections/screening of people, baggage, etc;		
9) Crew is not required to engage in inspection/screening of other crewmembers;		
10) Ensure the screening of all unaccompanied baggage;		
11) Ensure checked persons and their personal effects are segregated from unchecked persons;		
12) Ensure embarking passengers are segregated from disembarking passengers;		
13) Ensure a defined percentage of vehicles to be loaded on passenger vessels are screened before loading at the rate indicated in the VSP;		
14) Screen all unaccompanied vehicles to be loaded on passenger vessels prior to loading;		
<b>and</b>		
15) Respond to the presence of unauthorized persons onboard, including repelling unauthorized boarders.		
f) <b>MARSEC Level 2</b> - The additional security measures required may include the following:		
1) Increasing the frequency and detail of screening people/personal effects/vehicles being embarked, except for gov't-owned vehicles on official business with proper credentials for entry;		
2) X-ray screening of all unaccompanied baggage;		
3) Assigning additional personnel to patrol decks during periods of reduced vessel operations;		
4) Limiting the number of access points to the vessel by closing and securing some;		
5) Denying access to visitors who do not have a verified destination;		
6) Deterring waterside access to the vessel which may include the facility providing boat patrols; <b>and</b>		
7) Establishing a restricted area on the shore side of the vessel in cooperation with the facility.		
g) <b>MARSEC Level 3</b> - The additional security measures required may include the following:		
1) Screening all persons, baggage and personal effects for dangerous substances and devices;		
2) Performing one or more of the following on unaccompanied baggage:		
i) Screen unaccompanied baggage more aggressively, for example, X-ray from two or more angles;		
ii) Prepare to restrict or suspend handling unaccompanied baggage; <b>or</b>		
iii) Refuse to accept unaccompanied baggage onboard;		
3) Being prepared to cooperate with responders and facilities;		

4) Limiting access to the vessel to a single controlled access point;		
5) Granting access to only those responding to the security incident or threat;		
6) Suspending embarkation or disembarkation of personnel;		
7) Suspending cargo operations;		
8) Evacuating the vessel;		
9) Moving the vessel; <b>and</b>		
10) Preparing for a full or partial search of the vessel.		
<b>MARSEC Directives (Performance Standards)</b>		
Owner/operator must have procedures to verify screening rates described in the VSP. Rates may be measured over a reasonable time period determined by the CSO/VSO. The period should be noted in the VSP. Minimum rates for each MARSEC Level should be per the tables provided in appropriate Directive below, as applicable:		
104-1 Cruise Ship		
104-2 Passenger Vessel/Ferry		
104-3 Cargo/Towing/Other Commercial Vessel		
104-4 MODU/OSV Vessel		
<b>104.270 Security Measures for Restricted Areas</b>		
a) <b>General</b> - The Owner/Operator must ensure the designation of restricted areas in order to:		
1) Prevent or deter unauthorized access;		
2) Protect persons authorized to be onboard;		
3) Protect the vessel;		
4) Protect sensitive security areas within the vessel;		
5) Protect security and surveillance equipment and systems; <b>and</b>		
6) Protect cargo and vessel stores from tampering.		
b) <b>Designation of restricted areas.</b> Owner/Operator must ensure restricted areas are designated as specified in the approved VSP. Restricted areas must include, as appropriate:		
1) Navigation bridge, machinery spaces, and other control spaces;		
2) Spaces containing security and surveillance equipment, and their controls and lighting system controls;		
3) Ventilation and A/C systems, and other similar spaces;		
4) Spaces with access to potable water tanks, pumps or manifolds;		
5) Spaces containing dangerous goods or hazardous substances;		
6) Spaces containing cargo pumps and their controls;		
7) Cargo spaces and spaces containing vessels stores;		
8) Crew accommodations; <b>and</b>		
9) Any other spaces or areas vital to the security of the vessel.		
c) Owner/Operator must ensure that security measures and policies are established to:		
1) Identify which vessel personnel are authorized to have access;		
2) Determine which persons other than vessel personnel are authorized to have access;		
3) Determine the conditions under which that access may take place;		
4) Define the extent of any restricted area;		
5) Define the times when access restrictions apply; <b>and</b>		
6) Clearly mark all restricted areas and that unauthorized presence constitutes a breach of security.		

d) <b>MARSEC Level 1</b> - Owner/Operator must ensure security measures to prevent unauthorized access. Security measures may include:		
1) Locking or securing access points;		
2) Monitoring or using surveillance equipment;		
3) Using guards or patrols; <b>and</b>		
4) Using automatic intrusion devices to activate audible/visual alarm at a location continuously attended or monitored to alert vessel personnel to unauthorized access.		
e) <b>MARSEC Level 2</b> - In addition to measures taken at Level 1, additional measures may include the following:		
1) Increasing the frequency and intensity of monitoring and access controls on existing restricted access areas;		
2) Restricting access to areas adjacent to access points;		
3) Providing continuous monitoring of each area, using surveillance equipment; <b>and</b>		
4) Dedicating additional personnel to guard or patrol each area.		
f) <b>MARSEC Level 3</b> - In addition to measures taken at Levels 1 and 2, additional measures may include the following:		
1) Restricting access to additional areas; <b>and</b>		
2) Searching restricted areas as part of a security sweep of the vessel.		
<b>104.275 Security Measures for Handling Cargo.</b>		
a) <b>General</b> - Owner/Operator must ensure security measures related to cargo handling are specified in order to:		
1) Deter tampering;		
2) Prevent cargo not meant for carriage from being accepted and stored on the vessel;		
3) Identify cargo that is approved for loading onto the vessel;		
4) Include inventory control procedures at access points to the vessel; <b>and</b>		
5) When there are regular/repeated cargo ops with same shipper, coordinate security measures with the shipper/responsible party in accordance with established agreement and procedures.		
b) <b>MARSEC Level 1</b> - Ownr/Oprtr must ensure the implementation of measures to:		
1) Unless unsafe to do so; routinely check cargo and cargo spaces prior to and during cargo handling for evidence of tampering;		
2) Check that cargo to be loaded matches the cargo documentation or container numbers match shipping documents;		
3) Ensure in liaison with facility, that vehicles loaded on RO-RO and passenger ships are screened before loading as per frequency specified in VSP; <b>and</b>		
4) Check in liaison with facility, seals or other methods used to prevent tampering.		
c) <b>MARSEC Level 2</b> - Owner/Operator to ensure implementation of additional security measures which may include the following:		
1) Increase the frequency and detail of checking cargo and cargo spaces for evidence of tampering;		
2) Intensify checks to ensure that only intended cargo/containers or other units are loaded;		
3) Intensify screening of vehicles to be loaded on RO-RO and passenger vessels;		
4) In liaison with facility, increasing frequency and detail in checking seals and other methods to prevent tampering;		
5) Increasing frequency and intensity of visual and physical inspections; <b>or</b>		

6) Coordinating enhanced security measures with the shipper or other party i/a/w established agreement and procedures.		
d) <b>MARSEC Level 3</b> - In addition to measures at Level 1 and 2, additional measures which may include:		
1) Suspending loading or unloading of cargo;		
2) Being prepared to cooperate with responders, facilities, and other vessels; <b>or</b>		
3) Verifying the inventory and location of any hazardous materials carried on board.		
<b>104.280 Security Measures for Delivery of Vessel Stores and Bunkers</b>		
a) <b>General</b> - Owner/Operator must ensure security measures for delivery of stores/bunkers are implemented to:		
1) Check vessel stores for package integrity;		
2) Prevent vessel stores from being accepted without inspection;		
3) Deter tampering; <b>and</b>		
4) Prevent vessel stores and bunkers from being accepted unless ordered.		
b) <b>MARSEC Level 1</b> - Owner/Operator must ensure the implementation of measures to:		
1) Check vessel stores before being accepted;		
2) Check that stores or bunkers match the order prior to being brought onboard or bunkered; <b>and</b>		
3) Ensure stores are controlled or immediately and securely stowed following delivery.		
c) <b>MARSEC Level 2</b> - In addition to measures taken at Level 1, additional security measures may include:		
1) Intensify the inspection of vessel stores during delivery; <b>or</b>		
2) Checking vessel stores prior to receiving them onboard.		
d) <b>MARSEC Level 3</b> - In addition to security measures at Levels 1 and 2, additional security measures may include:		
1) Checking all vessel stores more extensively;		
2) Restricting or suspending delivery of vessel stores and bunkers; <b>or</b>		
3) Refusing to accept vessel stores onboard.		
<b>104.285 Security Measures for Monitoring</b>		
a) <b>General</b> -		
1) Owner/Operator to ensure the implementation of security measures by continuously monitoring through a combination of lighting, watch keepers, security guards, deck watches, waterborne patrols, auto intrusion-detection devices, or surveillance equipment of the following:		
i) Vessel;		
ii) Restricted areas onboard the vessel; <b>and</b>		
iii) Area surrounding the vessel.		
2) The following must be considered when establishing the appropriate level & location of lighting:		
i) Vessel personnel should be able to detect activities on & around vessel on both shore side & waterside;		
ii) Coverage should facilitate personnel identification at access points;		
iii) Coverage may be provided through coordination with the port or facility; <b>and</b>		
iv) Lighting effects (such as glare) and its impact on safety, navigation, and other security activities.		

b) <b>MARSEC Level 1</b> - Owner/Operator to ensure security measures that may be done in coordination with facility to:		
1) Monitor the vessel, particularly vessel access points and restricted areas;		
2) Be able to conduct emergency searches of the vessel;		
3) Ensure that equipment or system failures or malfunctions are identified and corrected;		
4) Ensure that automatic intrusion detection device sets off audible/visual alarm at location continuously attended or monitored;		
5) Illuminate deck and access points from sunset to sunrise to enable ID of persons seeking access to vessel; <b>and</b>		
6) Use maximum available lighting underway from sunset to sunrise consistent with safety and international regs.		
c) <b>MARSEC Level 2</b> - In addition to security measures at Level 1, additional security measures may include:		
1) Increasing the frequency and details of security patrols;		
2) Increasing the intensity and coverage of lighting, alone or in conjunction with facility;		
3) Using or increasing the use of security/surveillance equipment.		
4) Assigning additional personnel as security lookouts;		
5) Coordinating with boat patrols when provided; <b>or</b>		
6) Coordinating with shoreside foot or vehicle patrols; when provided.		
d) <b>MARSEC Level 3</b> - In addition to security measures at Levels 1 and 2, additional security measures may include the following:		
1) Cooperating with responders and facilities;		
2) Switching on all lights;		
3) Illuminating the vicinity of the vessel;		
4) Activating all surveillance equipment capable of recording activities on or in vicinity of the vessel;		
5) Maximizing the length of time such surveillance equipment can continue to record;		
6) Preparing for underwater inspection of the hull; <b>and</b>		
7) Initiating measures, i.e. slow revolution of propeller(s), to deter underwater access to the vessel hull.		
<b>104.290 Security Incident Procedures</b>		
For <b>each MARSEC Level</b> , the Owner/Operator must ensure the VSO & vessel security personnel are able to:		
a) Respond to security threats or breaches of security and maintain critical vessel and vessel-to- facility operations to include:		
1) To prohibit entry into affected area;		
2) Deny access to the vessel except to those responding to the emergency;		
3) Implement MARSEC Level 3 security measures throughout the vessel;		
4) Stopping cargo handling operations; <b>and</b>		
5) Notify shore side authorities or other vessels of the emergency;		
b) Evacuating the vessel in case of security threats or breaches of security;		
c) Reporting security incidents as required in 101.305;		
d) Briefing all vessel personnel on possible threats and the need for vigilance as well as soliciting their assistance; <b>and</b>		
e) Securing non-critical operations in order to focus response on critical operations.		

<b>104.292 Additional Requirements - Passenger Vessels and Ferries</b>		
a) At <b>all MARSEC Levels</b> , the Owner/Operator must ensure that security sweeps are performed prior to getting underway and after any period the vessel was unattended.		
b) As an alternative to ID checks and passenger requirements in 104.265 e) 1), e) 3), and e) 8), the Owner/Operator may ensure security measures are implemented that include:		
1) Searching selected areas prior to embarking passengers and prior to sailing; <b>and</b>		
2) Implementing one or more of the following:		
i) Performing routine security patrols;		
ii) Providing additional closed circuit TV's to monitor passenger areas; <b>or</b>		
iii) Securing all non passenger areas.		
c) Passenger vessels certificated to carry > 2000 passengers working in coordination with the terminal may be subject to additional vehicle screening requirements in accordance with a MARSEC Directive or other orders issued by the Coast Guard.		
d) Owners and operators of passenger vessels covered by this Part that use public access facilities (33 CFR 101.105) must address security measures for the vessel-public access facility interface per the appropriate Area Maritime Security Plan (AMSP).		
e) At <b>MARSEC Level 2</b> - Owner/Operator must ensure, in addition to Level 1 measures, the implementation of the following:		
1) Search selected areas prior to embarking passengers and prior to sailing;		
2) Passenger vessels certificated to carry < 2000 passengers may be subject to additional vehicle screening requirements in accordance with a MARSEC Directive or other orders issued by the Coast Guard; <b>and</b>		
3) As an alternative to the ID and screening requirements in Part 104.265 e) 3) and f)1) intensify patrols, security sweeps and monitoring identified in paragraph b) of this section.		
f) At <b>MARSEC Level 3</b> - Owner/Operator in addition to Levels 1 and 2, as an alternative to the ID checks and passenger screening requirements in Part 104.265 e) 3) , ensure that random armed security patrols are conducted, which need not consist of vessel personnel.		
<b>104.295 Additional Requirements - Cruise Ships</b>		
a) At <b>all MARSEC Levels</b> the Owner/Operator must ensure:		
1) Screen all persons, baggage and personal effects for dangerous substances and devices;		
2) Check the ID of all persons seeking to board the vessel; this check includes confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, govt ID etc;		
3) Perform security patrols; <b>and</b>		
4) Search selected areas prior to embarking passengers and prior to sailing.		
b) At <b>MARSEC Level 3</b> , the Owner/Operator must ensure that security briefs are given to passengers about the specific threat.		
<b>104.297 Additional Requirements - Vessels on International Voyages</b>		
a) An Owner/Operator of a U.S. flag vessel subject to SOLAS, 1974, must be in compliance with the applicable requirements of SOLAS Chapter XI-1, SOLAS Chapter XI-2 and the ISPS Code, Part A.		
b) Owners/Operators of U.S. flagged vessels that are required to comply with SOLAS must ensure an ISSC as provided in 46 CFR Parts 2.01-25 is obtained for the vessels. This Certificate must be issued by the Coast Guard.		



c) Owners/Operators of vessels that require an ISSC in para (b) of this section must request an inspection in writing at least 30 days prior to the inspection date to the OCMI of the port where the vessel will be inspected to verify compliance with this part and applicable SOLAS requirements. The inspection must be completed and the initial ISSC must be issued prior to July 1, 2004.		
<b>Subpart C - Vessel Security Assessment (VSA)</b>		
<b>104.305 Vessel Security Assessment (VSA) requirements</b>		
<b>d) VSA report.</b>		
1) Vessel Owner/Operator must ensure that a written VSA report is prepared and included as part of the VSP. The VSA report must contain:		
i) A summary of how the on-scene survey was conducted;		
ii) Existing security measures, procedures and operations;		
iii) A description of each vulnerability found during the assessment;		
iv) A description of security countermeasures that could be used to address each vulnerability;		
v) A list of the key vessel operations that are important to protect;		
vi) The likelihood of threats to key vessel operations; <b>and</b>		
vii) A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the vessel.		
2) The VSA report must address the following elements onboard or within the vessel:		
i) Physical security;		
ii) Structural integrity;		
iii) Personnel protection systems;		
iv) Procedural policies;		
v) Radio and telecommunication systems, including computer systems and networks <b>and</b> ;		
vi) The other areas that may, if damaged or used illicitly, pose a risk to people, property or operations onboard the vessel or within a facility.		
3) The VSA report must list the persons, activities, services, and operations that are important to protect, in each of the following categories:		
i) Vessel personnel;		
ii) Passengers, visitors, vendors, repair technicians, facility personnel, etc.;		
iii) Capacity to maintain safe navigation and emergency response;		
iv) Cargo, particularly dangerous goods and hazardous substances;		
v) Vessel stores;		
vi) Any vessel security communication and surveillance systems; <b>and</b>		
vii) Any other vessel security systems, if any;		
4) The VSA report must account for any vulnerabilities in the following areas;		
i) Conflicts between safety and security measures;		
ii) Conflicts between vessel duties and security assignments;		
iii) The impact of watch keeping duties and risk of fatigue on vessel personnel alertness and performance;		
iv) Security training deficiencies; <b>and</b>		
v) Security equipment and systems, including communication systems.		
5) The VSA report must discuss and evaluate key vessel measures and operations, including:		
i) Ensuring performance of all security duties;		
ii) Controlling access to the vessel, through the use of identification systems or otherwise;		

iii) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);		
iv) Supervising the handling of cargo and the delivery of vessel stores;		
v) Monitoring restricted areas to ensure that only authorized persons have access;		
vi) Monitoring deck areas and areas surrounding the vessel; <b>and</b>		
vii) The ready availability of security communications, information, and equipment.		
e) The VSA must be documented and the VSA report retained by the vessel owner or operator with the VSP. The VSA, the VSA report and VSP must be protected from unauthorized access or disclosure.		
<b>SOLAS Chap XI-2/6 Ship Security Alert System (SSAS)</b>		
1 Application		
2 The SSAS shall:		
2.1 initiate and transmit ship-to-shore alert to a competent Authority.		
2.2 not send the ship security alert to other ships.		
2.3 not raise any alarm on board the ship.		
2.4 continue the ship security alert until deactivated and/or reset.		
3 The SSAS shall:		
3.1 be capable of being activated from the navigation bridge and at least one other location.		
3.2 conform to performance standards not inferior to those adopted by the Organization.		
4 The SSAS activation points shall be designed so as to prevent inadvertent initiation.		
5 Equivalent SSAS compliance is radio installation meeting all standards of Chap IV.		
6 Administration notification of states		
7 Contracting Government notification of relevant Administration/States		
<b>Administrative:</b>		
<b>Enter the following information: (Overtyp e sample data)</b>		
Company address:		
John J Smith Inc.		
1234 Walkabout way		
Suite 16		
City, State 12345		
Vessel Name		
Official Number		
MISLE Activity Number		

**ENCLOSURE 2**

**33 CFR 104: GENERAL POLICY DISCUSSION**

**1. Overview**

The International Ship & Port Facility Security (ISPS) Code is the standard for vessel security that is applied to vessels that sail on international routes. The Coast Guard, as the representative of the Contracting Government<sup>1</sup>, must verify that the vessel fully complies with the ISPS Code prior to issuing the International Ship Security Certificate (ISSC). Regulations issued under the Maritime Transportation Security Act of 2002 (MTSA) require compliance for a vessel to operate but do not require a certificate to be issued. However, regulations mandated under MTSA, like ISPS Code, require the Coast Guard to verify that the vessel is in compliance with an approved security plan. Because domestic maritime security regulations encompass the requirements of the ISPS Code, compliance with 33 CFR 101-106 translates into compliance with ISPS for U.S.-flag vessels on an international route. The flow chart in Figure 1 outlines the overall process.

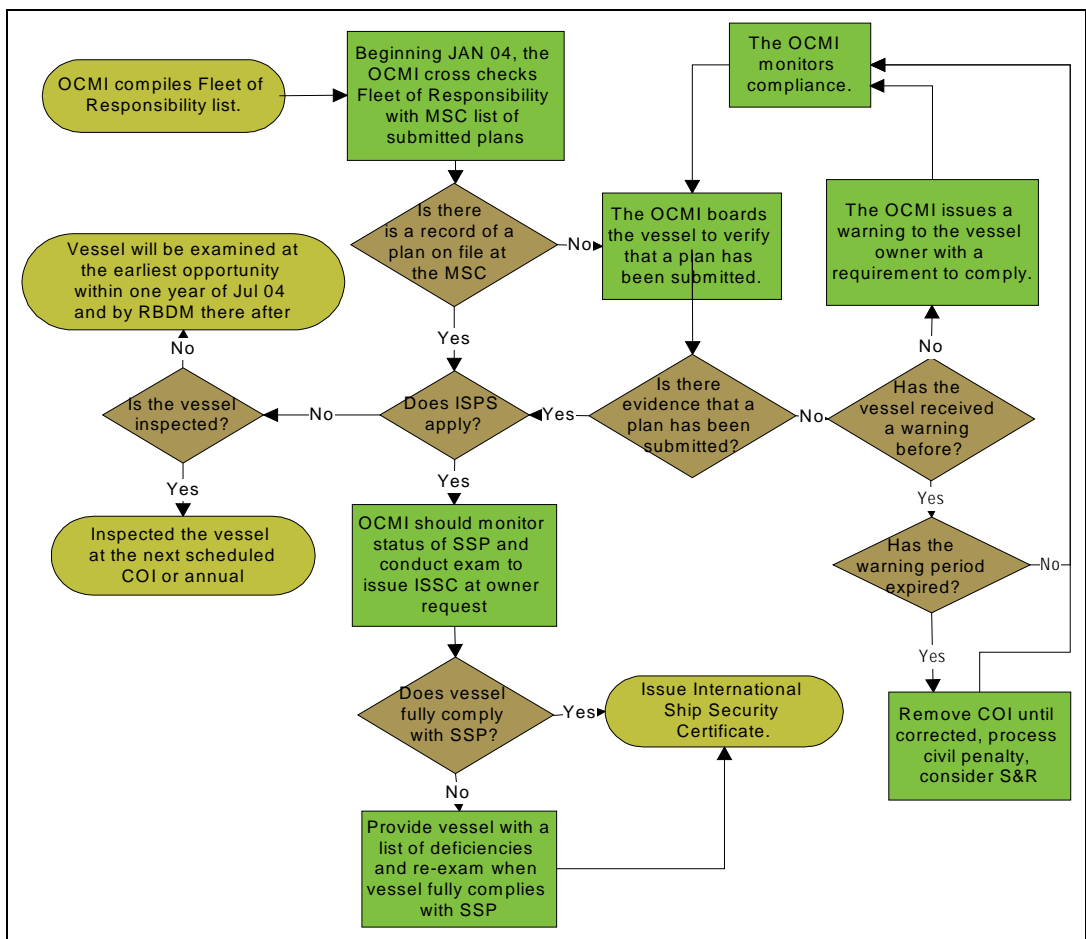
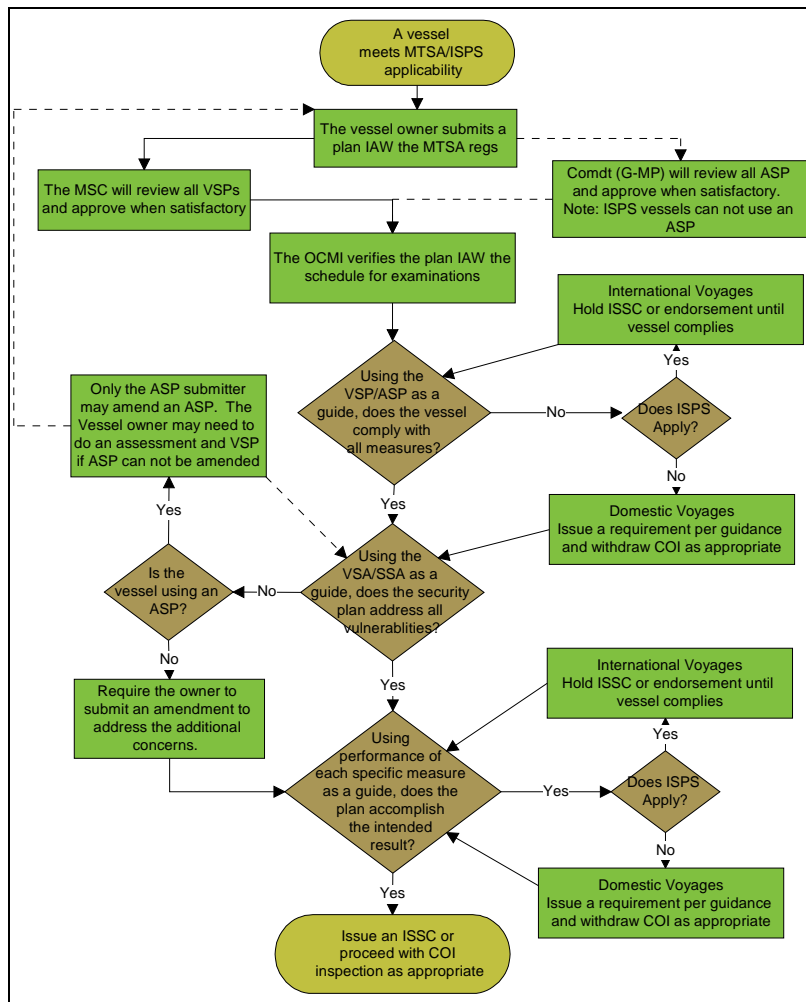


Figure 1

<sup>1</sup> The term “Contracting Government” used in the ISPS Code means the flag State, and for the purposes of this circular means the Coast Guard on behalf of the United States.

**2. Verification Process**

A. Regulations mandated by MTSA and the ISPS Code place the responsibility of completing an accurate security assessment and addressing the vulnerabilities in the Vessel Security Plan (VSP) or Ship Security Plan (SSP)<sup>2</sup> on the owner or operator of a vessel. The Coast Guard has the responsibility to verify that the vessel is complying with the approved plan. The three key steps of verification are to ensure the vessel complies with the VSP; ensure accuracy of the Vessel Security Assessment (VSA); and ensure that the measures in place adequately address the vulnerabilities. Each step in the verification process is an integral component in ensuring the overall security of a vessel and should occur concurrently as the inspector is completing the verification process. The flow chart in Figure 2 outlines this process.



**Figure 2**

B. Ensuring that the vessel complies with its approved VSP is the first step in the verification process. The VSP is the standard that the inspector will use to verify compliance on the vessel (e.g., if the VSP

<sup>2</sup> For the purposes of this circular, unless otherwise noted when the requirements for the Vessel Security Plan (VSP) or Vessel Security Assessment (VSA) are discussed, it includes the similar requirements for the Ship Security Plan (SSP) or Ship Security Assessment (SSA), respectively, which are required by the ISPS Code.

requires intrusion alarms on access points, the inspector will verify that the intrusion alarms are installed and working.) This process may be considered analogous to the process that the Coast Guard follows to verify compliance with other approved plans<sup>3</sup>. The approved VSP is checked for compliance with the required technical aspects during the review process, and it is inspector's task to compare the measures contained in the plan to the measures actually in place on the vessel. To prevent multiple returns for revision, MSC may issue approval letters with comments. The inspector will be required to check that these comments are addressed to their satisfaction by the owner/operator the same as is done by MSC when approving vessel safety plans.

- C. The next step is for the inspector to ensure that the VSA accurately addresses the security environment that exists on the vessel. The owner is responsible for conducting an accurate assessment that will be reviewed by the Coast Guard. An example of a situation is one in which the inspector verifies all measures outlined in the VSP are present but identifies a certain security vulnerability that is not addressed in the VSA (e.g., a ship storage space unaccounted for). Because the vulnerability is not identified in the assessment, the VSP would not specify a security measure for it. It is the inspector's duty to be vigilant for such vulnerabilities omitted from the VSA.
- D. Finally, the COTP/OCMI must also determine if the measure outlined in the approved VSP adequately addresses the security vulnerabilities identified in the VSA. This situation may occur when some exigent circumstance exists that was not accurately in the original assessment or, in the case of an Alternative Security Program (ASP), was not envisioned in the original plan. An example of such a situation would be if the VSP specifies intrusion alarms for an access point, but the devices that are installed and operating properly do not detect intrusion (i.e., the measure is in place and working, but does not perform the desired function). This is by far the most difficult step in the verification process and may require the COTP/OCMI to seek additional advise through the chain of command to Commandant (G-MP).
- E. These steps should occur concurrently as the inspector is completing the verification process. The requirements are performance based for the most part, and the evaluation of a given security measure should be judged based on its execution and effectiveness (i.e., if the measure can be done and does the job intended, it should be considered adequate). This circular is meant to offer policy to inspectors and to the industry that is useful during the VSP verification on the vessel. As with all policy, this guidance should not be considered as limiting in any way. Rather, the guidance contained herein should be considered as an example of satisfying the intent of the regulations.

### **3. Verification Cycle**

- A. The ISPS Code requires a vessel to conduct a Ship Security Assessment (SSA) and submit a Ship Security Plan (SSP) for approval to address all of the vulnerabilities that have been identified. The SSP must address the requirements found in Part A of the ISPS Code while also taking into account the provision contained in Part B. Once the plan is approved, the Contracting Government must do an on board verification that the vessel is in full compliance with the plan before an ISSC may be issued. From the deadline of 1 July 2004, no vessel subject to SOLAS XI-2 may operate without a valid ISSC. The VSP must be re-verified at the second or third annual exam, and resubmitted to the Contracting Government every five years.

---

<sup>3</sup> A copy of the approved plan must be on the vessel if manned or available if an unmanned vessel.

- B. Domestic regulations issued under MTSA similarly requires an assessment (VSA), a plan (VSP) and review every five years. However, although 33 CFR 104, Vessel Security, does require verification of the VSP, it does not require a separate certificate. Verification is incorporated into the inspection for certification process for vessel inspected in accordance with 46 USC § 2103, which will include a drill. Follow-up verifications will be conducted at the periodic exam and include a drill. Any deficiencies noted during an intervening inspection must be addressed immediately. Uninspected vessels must undergo verification, initially, at least once every five years, and based on risk at other times (i.e., high risk barge cargo in high consequence locations). Vessels to which both 33 CFR 104 and the ISPS Code applies should comply with 33 CFR 104 but submit an application for ISPS Code verification in accordance with 33 CFR 104.297.

#### **4. Verification Personnel**

- A. The verification of VSP and the ISPS Code requirements is a part of the inspection for certification on inspected vessels. An inspector conducting verification should possess the qualification of the type of vessel that is being verified (e.g., the verification of the VSP on a large passenger vessel should be conducted by an individual qualified to inspect Subchapter H vessels). The purpose of this is to ensure that the individual conducting the verification has experience on the particular class of vessel. Experience and an understanding of the vessels operations are essential in detecting potential vulnerabilities not addressed in the VSP.
- B. Aside from the qualifications above, the person conducting the verification should possess an understanding of 33 CFR 104 and the ISPS Code as appropriate. Ideally, the individual would have the same level of knowledge as that required of the Vessel Security Officer (VSO). Specific training requirements for an individual conducting a security verification is contained in separate guidance.

#### **5. Deficiencies**

- A. Deficiencies found during the verification process must be addressed immediately. A deficiency is a noncompliance with an approved VSP. A deficiency, like the non-compliance described in 33 CFR 104.125, is a condition in which the vessel is temporarily unable to comply with its approved VSP. An example of a deficiency would be on a vessel's VSP that specifies an intrusion detection alarm will protect each access point, but the device is inoperable. A deficiency is separate from a condition in which the vessel is in compliance with its VSP, but an issue exists that compromises the security of the vessel and requires an amendment to the VSP. An example of this situation might be in which the VSP specifies that each roving patrol will protect restricted areas. Yet, this measure is inadequate due to the ease of accessibility by unauthorized persons. In such a case the vessel is technically in compliance with its VSP, but the measure does not overcome the vulnerability.
- B. The severity of the deficiency must dictate the corrective action. On a vessel that sails on domestic voyages only, deficiencies may be considered in the same light as deficiencies with safety requirements. Some items that pose a minor risk may be addressed with a CG-835, while the severity of some deficiencies may be considered "no-sail" items. A minor item would be in which the safety and security of the vessel are not placed at direct risk. An example of a minor deficiency might be the failure of an individual surveillance camera, which can be replaced by a continuous sentry. When deciding the course of action to address a deficiency, the inspector should consider if a temporary measure might be employed to mitigate the risk (i.e., can a temporary substitute for the measure provide equivalent security). The complete failure of an entire security system that cannot be

duplicated or replaced with a substitute measure should be considered as a no-sail deficiency. An example of a no-sail deficiency would be failure of the surveillance system that leaves large areas of the vessel unsecured. Such a deficiency that poses a direct risk to the vessel, passengers, crew, or cargo requires the operations halted. If the vessel is uninspected, a Captain of the Port (COTP) order is issued to prevent operation of the vessel. The OCMI or COTP should be consulted when making this decision, but nothing should prevent the inspector from taking immediate action if the vessel is in immediate danger.

- C. If a requirement is issued for a deficiency, only the minimum amount of time to correct the situation should be allowed and only then if a substitute measure can be instituted that provides the same or great security. All deficiencies must be entered into Marine Information for Safety and Law Enforcement (MISLE).
- D. Vessels subject to the ISPS Code must not receive an ISSC and the ISSC must not be endorsed if a deficiency is detected during the verification process. However, items that are not part of the vessels approved plan, but which requires an amendment as described above should not preclude the vessel from receiving an ISSC, or endorsement. Items that are identified for an amendment must be documented in accordance with 33 CFR 104.415.

## 6. Documentation

- A. Documentation of the VSP verification is essential to effective program management. The MISLE system is the Coast Guard's official database for tracking marine safety, security, and law enforcement information. Timely input will assist OCMI's and COTPs in tracking compliance. The process for tracking the specific verification actions and events are contained in the MISLE user guide. You can access several MISLE user guides by visiting MISLENET on the Web: [http://mislenet.osc.uscg.mil/user\\_guides.aspx](http://mislenet.osc.uscg.mil/user_guides.aspx).
- B. Vessels that are subject to SOLAS chapter XI-2 must possess a valid ISSC to operate on an international voyage. The ISSC (CG-4360) has been published in the Coast Guard's forms library in Adobe format. Manual input of information is required, and an "image" should be captured in MISLE each time the ISSC is issued, reissued, or amended. The activity number found at the top of the form should correspond to the activity number in MISLE when issued.
- C. A vessel that must possess an ISSC must also maintain a Continuous Synopsis Record (CSR). The CSR contains all of the information regarding the operation particulars of the vessel. Specific question regarding the CSR should be referred to the National Vessel Documentation Center (NVDC), which is the centralized location for processing the CSR. Required changes to the CSR must be processed, and an amended form issued by the Coast Guard within 90 days. Although not a part of the ISPS Code, the inspector should closely examine the information contained on the CSR to ensure its validity. Any discrepancies between the CSR and other valid documents must be corrected immediately. The inspector should point out the discrepancy to the master of the vessel for immediate action.
- D. An inspected vessel that is not on an international voyage and does not require an ISSC will not be issued a separate certificate or endorsement on its COI. The 33 CFR part 104 requirements are incorporated into the certification process. A valid COI is evidence of compliance with 33 CFR 104. A permanently moored vessel not certificated is not required to comply with 33 CFR part 104 but may be regulated under 33 CFR part 103. As discussed above, a deficiency may be documented on a



CG-835 with a compliance date set at the minimum amount of time required to correct it. All deficiencies must be recorded in MISLE.

- E. Security plan verifications on uninspected vessels may be documented with the Uninspected Towing Vessel Examination Report (figure 1) contained in this enclosure or a locally generated form that contains the same information. The form will serve as an on board record of the plan verification and document other deficiencies as required. The verification process is the substantially the same for Uninspected Towing Vessels (UTV) as for inspected vessels. A cursory examination of critical safety equipment will be incorporated and documented on the UTV Exam form. Specific guidance of the scope and content of the safety portion of the exam is provided in separate guidance. The inspector should leave a copy of the UTV Exam form with the vessel's master and forward the results of the exam to the owner along with any requirements in writing.
7. **Appeals** The appeal process for vessel owners that wish to challenge an OCMI/COTP decision may follow the course found in 33 CFR 101.420. The Commandant (G-MOC) has the final agency action for security compliance appeals. Appeals of any decision made regarding the actual plan approval by the MSC should be directed to Commandant (G-MP). Specific guidance for the appeal process is contained in separate guidance.
8. **International Voyages** Regardless of when the voyage began, any SOLAS vessel (i.e., meets the service and/or tonnage criteria) that is operating in the waters of a foreign country will be considered to be on an international voyage, that was begun in a port in of the United States, and therefore is subject to the ISPS Code.

**Uninspected Towing Vessel (UTV) Examination Report**

1 Date of Exam: \_\_\_\_\_ VIN: \_\_\_\_\_

Vessel Name: \_\_\_\_\_

Location: \_\_\_\_\_

This vessel is / is not in compliance with an approved Vessel Security Plan. (**Circle one.**)

The following deficiencies were noted during the exam:

<u>Deficiency</u>	<u>Cite</u>	<u>Action Required and Time Allotted</u>
1. _____ _____ _____	_____ _____ _____	_____ _____ _____
2. _____ _____ _____	_____ _____ _____	_____ _____ _____
3. _____ _____ _____	_____ _____ _____	_____ _____ _____
4. _____ _____ _____	_____ _____ _____	_____ _____ _____
5. _____ _____ _____	_____ _____ _____	_____ _____ _____

All deficiencies must be corrected within the time allotted.

\_\_\_\_\_  
Inspector

\_\_\_\_\_  
Vessel Security Officer or Master

**This form should be retained on board as a record of this exam.**

**ENCLOSURE 3**

**DISCUSSION OF SPECIFIC REQUIREMENTS OF 33 CFR 104**

**1. Instructions for Using This Guide**

- A. The implementation guidance follows the structure of the regulations, which is laid out the same for vessel, facilities, and Outer Continental Shelf (OCS) facilities. Except where noted, the same background and application information can be used regardless of where the inspection is taking place. For example, the waiver requirements are the same for a vessel as an OCS facility.
- B. This guidance applies to foreign vessels that are not subject to SOLAS that operate with a Vessel Security Plan approved by the Coast Guard. Foreign vessels subject to SOLAS will be addressed under a separate Port State Control NVIC.
- C. In each paragraph, there is a background section in plain type, followed by the practical application in italics. The background section is intended as a general discussion of the particular regulation cite. Other background information is contained in enclosure (4), which is derived from the preamble of 33 CFR 104. The background information contained in this enclosure is directed at answering an inspector's concerns for completing VSP verification rather than the more general information contained in the preamble.
- D. The italicized portions give specific direction for the inspector to use when verifying compliance. The purpose of the inspection is to verify that the vessel is complying with the approved plan and to identify possible security vulnerabilities that are not adequately addressed. When making these judgments the inspector may use the guidance in the italicized portion of this enclosure. As with any policy guidance, the information contained herein is not a regulation and does not impose legally-binding requirements on any party. The owner or operator crew may suggest an alternative to this guidance that meets or exceeds these standards, and the alternative may be considered at any time.

**2. Compliance documentation.**

**33 CFR 104.120**

An approved VSP shall be accompanied by a letter of approval from the Marine Safety Center (MSC) dated within the last five years. Amendments and revisions to the Vessel Security Plan (VSP) should follow the process outlined later in this NVIC.

Inspectors may ensure the validity and accuracy of compliance documentation during the course of vessel inspections.

When the VSP is not approved, the attending inspector may verify the existence of an acknowledgement letter from the MSC stating that the plan is currently under review or through a cross check of the approval date in MISLE. The vessel may continue to operate so long as it is in full compliance with the submitted plan.

For a vessel operating under an Alternative Security Program (ASP), the inspector should verify that a copy of the Coast Guard approved ASP is available and that it includes the following:

- *A specific security assessment report.*
- *A letter from the owner or operator certifying which ASP is being used, and that the facility or vessel is in full compliance with that program.*

*Foreign Vessels:*

*For foreign vessels not subject to SOLAS Chapter XI, the inspector may verify the following:*

- *A valid letter from the MSC attesting that a VSP substantially in compliance with the content requirements of 33CFR104 has been submitted.*
- *An approved ASP along with a letter from the master that the vessel is in full compliance with the security plan may also be accepted.*
- *A valid International Ship Security Certificate (ISSC).*

*Unmanned Vessels:*

Approval letters (for VSPs or ASPs) for unmanned vessels are required by regulation to be carried on board and readily accessible. However, as required by regulation, the VSP/ASP should not be maintained on board the vessels but must be maintained in a secure location. During *scheduled* inspections, the plans must be made available to the Coast Guard upon request.

*When scheduling inspections, the inspector should coordinate with owner/operators to ensure VSP/ASP availability at the time of inspection.*

*Alternate Compliance Program (ACP) Vessels*

Vessels that are enrolled in the ACP are issued a certificate by the Coast Guard and are examined annually. Although ISPS allows the flag Administration to authorize a Recognized Security Organization (RSO) to issue an ISSC, 33 CFR 104 does not. All U.S.-flagged vessels must have their VSP verified by the Coast Guard in order to have an ISSC issued or endorsed.

*Inspectors may follow the guidance contained in the ACP NVIC for further guidance.*

*International Ship Security Certificate (ISSC) (U.S. SOLAS Vessels only):*

This document will be issued by the local OCMI following a satisfactory initial, or renewal verification of the VSP. The certificate carries a 5-year expiration date and has a minimum provision for one periodic verification.

Continuous Synopsis Records (CSR) (U.S. SOLAS Vessels only):

The USCG issues the CSR to U.S.-flag vessels subject to the ISPS Code. It provides a historic “snapshot” of pertinent vessel information such as official number, port of registry, charterer, and classification information.

*The CSR should be accurate and reflect current vessel information. Updates to vessel files may be required. Discrepancies found in the CSR should be reported to the vessel master and/or owner so that corrective actions can be taken.*

**3. Noncompliance.**

**33 CFR 104.125**

When a vessel must temporarily deviate from the requirements of an approved VSP, the owner or operator must notify the cognizant COTP and either suspend operations or request and receive permission from the COTP to continue operating. An example of noncompliance is when the VSP specifies that an intrusion alarm must be in a certain space but the alarm is inoperable. The owner or operator in this case may request to cease operations or propose an alternative, such as a guard .

*A noncompliance may be viewed as being similar to a deviation from the 33 CFR 164 regulations. The COTP must decide if noncompliance represents a significant risk, and issue a COTP order to suspend operations or give COTP written authority to continue operations. If the condition is to persist while the vessel is transiting other COTP zones, each COTP or, in cases covered under 33 CFR 106.120, the cognizant District Commander, may agree to the measures imposed, consider additional measures, or prohibit entry until the deficiency is corrected. See enclosure (1) of this circular.*

**4. Waivers.**

**33 CFR 104.130**

Waivers are not temporary deviations and are requested for exceptions to a security regulation based on what the owner or operator considers unnecessary in light of the nature or operating conditions of the vessel, facility, or OCS facility prior to operating. Ideally, such a request would be made before the plan is submitted, since the waiver must be granted before operation. An example of a waiver might be if the vessel owner believed access control measures to be unnecessary due to the unique design and operation of the vessel. The Commandant (CG-543) may require the vessel owner or operator to provide data for use in determining the validity of the requested waiver, such as diagrams, pictures, or other reports. The data collected would be used to determine if the waiver could be reasonably granted without exposing the vessel to unacceptable risk. If warranted, the Commandant (CG-543) will grant a waiver in writing but may impose conditions that must be followed.

*The inspector will need to examine the waiver approval letter to verify that any conditions expressed are implemented. Since the conditions placed on the waiver are meant to ensure the overall security of the vessel, the letter must be fully implemented. A vessel that is using an ASP is not eligible to request a waiver since the regulations require an ASP plan to be implemented in its entirety.*

**5. Equivalents.**

**33 CFR 104.135**

The vessel owner or operator may propose an equivalent to any requirement. An equivalent is a substitute for a required security measure and may be granted by Commandant (CG-543) as long as the overall security of the vessel is not compromised. Equivalent security measures requested under this paragraph would not address temporary security deficiencies, which are covered under “noncompliance.” The equivalent measure must meet or exceed the required measure in order to be granted. An example of an equivalent measure might be when the vessel owner believes that the unique design or operation of the vessel’s access control measures are performed through some other function of the vessel, without a specific measure needed to address this concern.

*The inspector will need to examine the approval letter of any equivalencies that may exist. Equivalencies granted after the security plan has been approved should be noted in an amendment to the plan. Vessels that are using an ASP may not use an equivalency since the regulations require the ASP plan to be implemented in its “entirety.”*

**6. Alternative Security Programs (ASP).**

**33 CFR 104.140**

A. Vessels operating under the auspices of an approved ASP are required to address the relevant areas cited in 33 CFR 104. However, the ASP provision of the rule has provided a mechanism by which segments of the maritime industry, through application by the industry associations or other representative groups, are able to tailor their program to the unique functions inherent of their specific operations. The result is a set of relevant, performance-based security measures for the industry groups choosing to utilize an approved ASP. For this reason, the inspector of a vessel using an approved ASP may find that certain language or security measures contained in some parts of the rule will differ from the language or security measures listed in the ASP. An example would be the requirement in 33 CFR 104.265 (e) (3) that vessels check the identification of any person seeking to board the vessel at MARSEC Level 1. In an ASP, the approval authority may take into account the availability of video monitoring capable of facial feature recognition and recording and approve this as satisfying the intent of the requirement for individual identification. Additionally, an industry or group may determine that a section of the regulation is not applicable to their operations. For example, a passenger vessel group may state in their ASP that they do not need to address 33 CFR 104.275 or 33 CFR 105.265, respectively – security measures for handling cargo – because they do not handle cargo of any type.

B. Individual owner/operators who have subscribed to an ASP are not eligible for the application of equivalent security measures (33 CFR 101.130) or waivers (33 CFR 104.130 or 33 CFR 105.130). The ASP approved for their parent organization is a *de facto* equivalency for the Vessel Security Plan and no other equivalent security measures should be in place. Likewise, approved ASP’s must be implemented in their entirety (see 33 CFR 101.120 (b) (2)) so waivers or additional equivalents are not appropriate.

- C. Should an enforcement inspection reveal that an owner/operator has correctly implemented an approved ASP in its entirety but security vulnerabilities exist in the vessel operation, the COTP shall be advised. Under 33 CFR 104.415(a)(ii) for vessels or 33 CFR 105.415(a)(ii)(f), the Coast Guard can determine that an amendment is necessary and advise the organization that submitted the ASP for approval accordingly. Following such notification, it will be necessary for the original submitting organization to provide their proposed amendment to the Commandant (CG-543) for review and approval. If the submitting organization does not wish to amend the ASP, the vessel owner must submit a VSP for the vessel to the MSC.

*An inspector of a vessel covered under an Alternative Security Program (ASP) approved by the Commandant (CG-543) should find a copy of the ASP and the vessel specific security assessment report on site. In addition, there should be a copy of the letter sent by the company to the appropriate plan approval authority identifying which ASP they have implemented, which vessels are covered and attesting that they are in full compliance with the ASP. It will be the responsibility of the individual performing the on-site inspection to confirm that the vessel is in compliance with the Alternative Security Program as it was approved, including any conditions of approval stipulated by the Commandant (CG-543) in its entirety. If the copy of the ASP onboard is the original "template" and no information is filled in, there should be a separate "VSP" generated to address the requirements outlined in the ASP.*

*In those cases where both the vessels and the facilities serving those vessels are owned and/or operated by the same entity, an alternative plan may recognize that the same party is responsible for security in both areas and approve an approach that addresses vulnerabilities and mitigation strategies for the vessels and the facility under one ASP. Therefore, the inspector will not be using separate plans for the vessels and the facility to determine compliance and, likewise, will not see some citations addressed in the plan if they are redundant between 33 CFR 104 and 33 CFR 105.*

## **7. Maritime Security (MARSEC) Directive.**

**33 CFR 104.145**

- A. As provided for in 33 CFR 101.405, the Coast Guard may issue MARSEC Directives that are used to provide vessels with objective performance standards such as access control or the secure handling of cargo. These directives will play a vital role in the successful implementation of 33 CFR 104 in many ways.
- B. MARSEC Directives will allow the Coast Guard to strike a balance between the need to communicate with the maritime industry while ensuring that our communications are secure. Since these directives are designated as Sensitive Security Information (SSI), the Coast Guard can communicate these objectives performance standards, such as the specific percentages of passengers or cargos that must be screened, while ensuring that such information is not subject to full public disclosure. MARSEC Directives allow the Commandant to ensure that there is consistency between COTP zones when enforcing the provisions of 33 CFR 104 by providing COTPs objective standards by which the performance of vessels nationwide shall be evaluated. MARSEC Directives allow the



Coast Guard the flexibility to tailor objective performance standards to the prevailing threat environment or industry segment. For example, if high capacity ferry vessels are at a greater risk for a Transportation Security Incident (TSI), the Coast Guard may issue a directive that would require enhanced security measures typical of a higher MARSEC Level that would apply only to that segment of the maritime industry.

- C. When a new MARSEC Directive is issued, the Coast Guard will publish a notice of the issuance in the Federal Register and through other means (i.e. local notices to mariners, press releases). The MARSEC Directives will be individually numbered and assigned to a series that corresponds with the part of this subchapter to which the MARSEC Directive refers. For example, the first MARSEC Directive addressing a new requirement for vessels regulated under 33 CFR 104 of this subchapter would be identified as MARSEC Directive 104-01. Upon receiving notice that a new MARSEC Directive has been issued, affected entities would contact or be contacted by their local COTP (or, if appropriate, their District Commander) to receive a copy of the MARSEC Directive. The COTP or District Commander will confirm, prior to distributing the MARSEC Directive, that the requesting entity is a person with a need to know, and that the requesting entity will safeguard the MARSEC Directive as SSI in accordance with 49 CFR 1520.
- D. Thus, continuing with the example of the previous paragraph, upon receiving notice that a MARSEC Directive in the 33 CFR 104 series has been issued, owners and operators of vessels covered by 33 CFR 104 of this subchapter would need to contact their local COTP to obtain a copy of the MARSEC Directive. They would then be required to comply with the MARSEC Directive, or follow the procedures set out in the MARSEC Directive for gaining approval of an equivalent security measure.
- E. Once a MARSEC Directive has been issued, it is the responsibility of the affected entities to comply with the Directive and as required by 33 CFR 104.240(b)(2) and 101.300(c) to notify the local COTP or District Commander, as appropriate, when compliance with the higher MARSEC Level has been implemented.

*Inspectors must have a thorough knowledge of the MARSEC Directives that have been issued, and how they may affect the vessels in their respective COTP/OCMI zones. It will be incumbent upon the inspector to ensure that vessels that are affected have incorporated the MARSEC Directives into their security plans and measures.*

**8. Company Security Officer (CSO).**

**33 CFR 104.210**

The CSO may delegate vessel security duties required under this part, but the CSO remains responsible for the performance of those duties.

*If a company has multiple CSOs, or if the CSO has delegated the duties in accordance with the regulations, the inspector may make inquiries of the CSO or designated crewmember to ensure that the CSO or designated crewmember understand their CSO responsibilities and that the ultimate responsibility rests with the CSO. In particular, an effective communication arrangement would be necessary to comply with the intent of the regulations. To validate*

*that the CSO can demonstrate satisfactory knowledge of the VSP, the inspector may ask the CSO the following questions:*

- *Describe the security organization of the company and its vessels.*
- *Describe how you keep your company's vessels apprised of changing security levels.*
- *Describe any problems or deficiencies that have been identified during annual audits.*

**9. Vessel Security Officer (VSO).**

**33 CFR 104.215**

VSO training is not mandated; instead, the regulations require that the VSO meet certain qualification requirements. These qualification requirements can be derived from formal (classroom) or on the job training.

*Inspectors may evaluate the ability of the VSO to perform the required duties and responsibilities in relation to other assignments within the organization, multiple facility assignments, and retention of responsibility for delegated duties.*

*The inspector will accept the following documents to confirm that the VSO meets the qualification requirements in 33 CFR 104.215 and the training requirements in the International Ship and Port Facility Security (ISPS) Code:*

- a) A course completion certificate from a VSO course; or*
- b) A letter from a senior company official that the person has met the knowledge requirements in 33 CFR §104.215(b) through job experience.*

*Inspectors may measure the performance of the VSO by interviewing relevant personnel, reviewing records and documents required under this part, observing drills and exercises, and reviewing or monitoring actual incidents.*

**10. Company and Vessel Personnel with Security Duties.**

**33 CFR 104.220**

The regulation requires members of the crew with security-related duties to possess a minimum level of knowledge. This knowledge may be derived from formal or on the job training. The crewmembers that perform the security duties on the vessel are the most important link in the security of the vessel. They are the “eyes and ears” that will either detect a potential security incident or fail to recognize it. The success or failure of the security plan will depend on them.

*The inspector may ask the crew to verify their knowledge of the required information through observation, and conversations with the crewmembers regarding the security responsibilities of the pertinent crew. The questions may be kept informal, but should probe the depth of knowledge that individuals possess concerning their assigned job. The questions may be directed at the security threats that the person may be expected to encounter, such as what type of behavior(s) would be considered “suspicious” when passengers are boarding the vessel. Although the average crewmember does not need to and should not know the entire security plan, the ability to identify the CSO, or VSO, and the aspects of the security plan that pertain to his/her station would demonstrate sufficient knowledge of the relevant sections.*

**11. Security Training for All Other Vessel Personnel.**

**33 CFR 104.225**

Security training for personnel other than those with security-related duties should be similar to safety orientation for non-crewmembers. The training should be relevant to the circumstances. For example, a contractor on board for a maintenance visit for a particular day may require only a short brief on the security measures in place and the restricted areas that cannot be accessed. Technical representatives working around a vessel for an extended period may be given more in-depth information including a briefing on specific threats and awareness measures.

*The inspector may verify that persons other than the crew on a vessel are adequately trained by direct observation and questioning, but at a reduced level from the crew. The inspector should also make use of personnel training records required under separate regulations.*

**12. Drill and Exercise Requirements.**

**33 CFR 104.230**

- A. During a verification, the inspector will witness a drill to ensure that the VSO is conducting a drill that tests the training of the crew, that the measures outlined in the VSP are executed correctly, and that these measures adequately address security threats. The success of a drill is somewhat subjective. However, certain goals should be accomplished by a drill in order to be successful, which might include the following:
- The measures contained in the VSP are fully implemented.
  - Correct actions are taken by the crew and others on board.
  - The VSO demonstrates effective control and communication.
  - The situation reaches a positive resolution.
- B. In order to evaluate the state of training on the vessel, the inspector should witness a drill selected at random. A drill scenario may be based on the security measures contained in the VSP. Prior to conducting the drill, the inspector should carefully review the procedures contained in the security plan for dealing with a particular security incident. The inspector should discuss the details with the VSO prior to beginning the drill. The inspector should also review the drill log to ensure that any best practices or lessons learned are taken into account. Ideally, the VSO will create a scenario that provides enough realism to challenge the crew's response. On an unmanned barge, it is not necessary to conduct a drill if the log shows that drills have been conducted in accordance with the plan.
- C. One example of a security drill cited in the regulations is for an unauthorized entry. The configuration of each vessel is unique and must be reflected in the security plan. The regulations contain specific examples of threats and vulnerabilities that should be considered when conducting the drill. However, other vulnerabilities may be identified when the plan is exercised during a drill (e.g. an access point or weakness enforcing control not envisioned in the plan).
- D. The regulations allow a company operating several similar vessels to hire new crewmembers, have them participate in a drill on board one vessel, and then rotate those crewmembers to

any of the similar vessels within that same company's fleet. For the purposes of these regulations, "similar" may be interpreted to mean any vessel in the company's fleet that has a VSP with essentially the same security measures. A ferry line, for example, that operates both high-speed craft and displacement vessels may have similar VSPs, even though the vessels are not "similar" in design. It is the responsibility of the VSO to ensure that all personnel are adequately trained, and in this case, that new personnel from a similar vessel are familiar with the particulars of the VSP that are unique to the vessel.

- E. Security drills and exercises may be combined with existing non-security drill and exercise requirements to increase efficiency. These may include safety, Area Maritime Security (AMS), and disaster preparedness drills. To be counted as a "drill" or "exercise" for the purposes of this part, the event must be in compliance with the definitions of a drill or exercise as stated in 33 CFR 101.105; test the response to security threats and incidents; and take into account the type of vessel operation, personnel changes, and other relevant circumstances.

*The inspector should critique the drill with the VSO and discuss corrective action, if necessary, to address any deficiencies noted. Any deficiencies with the VSP detected during the drill may be corrected by directing the owner in writing to submit an amendment per the regulations. Such a requirement should be allowed at least 60 days.*

*The inspector may accept proof of participation in an Area Maritime Security exercise to meet the requirement for an annual exercise if the owner furnishes proof of participation.*

### **13. Vessel Record Keeping Requirements.**

**33 CFR 104.235**

Inspectors should ensure that the VSO maintains the required records for security related evolutions such as training, drills and exercises, security threats, and maintenance of security equipment. These records may be kept in paper or electronic format and must be protected from unauthorized access or disclosure. The ISPS Code, part A, requires that vessels subject to ISPS maintain records on board the vessel (Note: from Preamble). All other vessels record categories (except the Declaration of Security (DoS) on manned vessels) need not be stored onboard but must be made available to the Coast Guard upon request.

### **14. Maritime Security (MARSEC) Level Coordination and Implementation.**

**33 CFR 104.240**

- A. The Secretary of the Department of Homeland Security sets the Homeland Security Advisory System (HSAS) threat condition; the Commandant will change MARSEC levels to match the HSAS level.
- B. An exception to this rule is provided for the COTPs to temporarily raise the MARSEC level in their zone to address an immediate threat to the Maritime Transportation System (MTS) when the immediacy of a threat or incident does not allow sufficient time to notify the Commandant. COTPs should only exercise this authority in the most immediate and urgent circumstances. Such circumstances would include immediate action to save lives,

mitigate great property damage or environmental damage resulting from a TSI, and if timely prior notification to the Commandant is not possible. If such a circumstance does arise, the COTP must immediately inform the Commandant via the chain of command. The heightened MARSEC level will only continue as long as necessary to address the serious threat which prompted the raised level.

- C. Changes in MARSEC levels shall be announced and implemented in the most expeditious means possible, preferably through a Broadcast Notice to Mariners or other existing mechanisms of communications (i.e., maritime exchanges, VTS, VTIS programs). Whatever means is used, it should be sufficient to provide timely and adequate notice to the regulated maritime industry.

*Inspectors need to be aware of the prevailing MARSEC Level before they visit a vessel, as this will determine which security measures will be in place at the time of inspection. For example, if the port is at MARSEC Level 2 or 3, the vessel should have in place all the security measures required by their plan for MARSEC Level 1 plus the measures required by the higher MARSEC Levels.*

**15. Communications.**

**33 CFR 104.245**

As per the regulations, these systems must be able to both effectively and continuously communicate with a wide variety of audiences not limited to facility and vessel personnel, shore authorities, other vessels, and national and local authorities. Systems may incorporate a range of means including telephones, radios, cellular phones, etc.

*Inspectors should examine the communication systems and procedures established under the VSP. Inspectors may question the VSO to ascertain the adequacy of provided communication equipment and procedures; testing may be necessary. Communications will be considered effective if the VSO can demonstrate sufficient operation.*

**16. Declaration of Security (DoS).**

**33 CFR 104.255**

Vessels are required to implement a DoS in coordination with the facility (including OCS facility) or another vessel. The DoS is the primary plan for shared security concerns and is required to remain in place throughout the time a vessel is moored at the facility or for the duration of the vessel-to-vessel interface. All vessels and facilities required to comply with 33 CFR parts 104, 105, and 106, must, at a minimum, comply with the DoS requirements of the MARSEC level set for the port. The vessel owner or operator must, for each vessel, ensure that adequate coordination of security issues takes place between the vessel and facility to include the execution of the DoS. Execution implies a greater degree of action than simply signing the document. Thus, vessels must implement the vessel's share of the DoS security measures before commencing to embark or disembark passengers, transfer of cargo or vessel stores.

*Inspectors should ensure adequacy of procedures for handling requests for a DoS; they should also review current and historical records for adequacy of a DoS, including signatures of VSO, FSO, their designated representatives and the current MARSEC level.*

*Inspectors should also observe vessel and facility operations to ensure compliance with the DoS.*

*In addition, inspectors should verify that continuing DoSs have not exceeded the maximum time periods (90 days for MARSEC 1, 30 days for MARSEC 2 and no continuing DoS authorized for MARSEC 3).*

**17. Security Systems and Equipment Maintenance.**

**33 CFR 104.260**

*Inspectors should review records related to inspection, testing and calibration of security equipment as well as the frequency of related actions to ensure that these are being conducted. Records available for review and consultation should include, but are not limited to, manufacturers maintenance recommendations, system plans or schematics, test records/logs, and deficiencies/system failures with repair and/or RSO repair documentation. Inspectors are encouraged ask the VSO questions related to inspection, testing, calibration, and maintenance of security equipment. Inspectors may also question the VSO and other personnel with security duties on how the system and subsystems work, including a demonstration of system functionality and any appropriate tests/alerts.*

**18. Security Measures for Access Control.**

**33 CFR 104.265**

*Inspectors may observe procedures in place to deter unauthorized access of people and the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports and whether security personnel show competence in their duties. Passenger vessels and ferries may comply with the measures contained in 33 CFR 104.292. Inspectors should cite the approved Security Plan and verify that the security measures specified for the current MARSEC level are in effect and deemed adequate. These measures include, but are not limited to, access points examined (gates, gangways, ramps, piers), identification procedures (personnel, vehicles, vendors), and entry restrictions/prohibitions regarding access to the vessel (guards, fences, checkpoints, etc). In addition to the current MARSEC level, measures for other MARSEC levels should be examined. Inspectors should question VSOs and other personnel with security duties regarding additional security measures for elevations in MARSEC level requirements as specified in their specific Security Plan. This includes, but is not limited to additional personnel, equipment, further limitations on access, and additional screening procedures. As an example, additional measures may include limiting the number of access points, deterring waterside access, suspending operations, and evacuation measures. The inspector should verify that the VSP addresses security measures for periods when the vessel is unattended, such as for daytime only operations.*

**19. Security Measures for Restricted Areas.**

**33 CFR 104.270**

Restricted Areas are designated in the VSP. The regulations contain the minimum areas that must be designated as restricted areas, but the owner may designate any location as a restricted area if deemed necessary.

*Inspectors may observe procedures in place to prevent and deter unauthorized access to*

*those restricted areas identified in the VSP. These areas include, but are not limited to, storage and supply sites, shore areas immediately adjacent to each vessel moored at a facility, areas containing critical infrastructure/equipment (power, water, command/control, etc.), and locations designed for loading cargo. Inspectors should cite the approved VSP and verify restricted area status for the current MARSEC level is in effect and deemed adequate. This includes, but is not limited to, the verification of locks or secured access points, locations properly marked and identified as restricted areas, surveillance equipment, and guards or patrols. Inspectors should question VSOs and other personnel with security duties regarding additional restricted area security measures for elevations in MARSEC level requirements as specified in their VSP. This includes, but is not limited to additional personnel, equipment, further limitations on restricted areas, and additional surveillance procedures. Nothing in this section should compromise the safety of the vessel, crew, or passengers (i.e., locks that block emergency escape scuttles).*

**20. Security Measures for Handling Cargo.**

**33 CFR 104.275**

*Inspectors may observe procedures in place to ensure the security of cargo handling operations and whether security personnel show competence in these duties. Inspectors should cite the approved VSP and verify that the Cargo Handling Security Procedures for the current MARSEC level are in effect and deemed adequate. These procedures include, but are not limited to, deterrence of cargo tampering, identification of unauthorized cargo (e.g., inventory control), and checking cargo for dangerous or unauthorized substances. In particular, a vessel's inventory procedures (logs, etc.) should be examined to ensure all HAZMAT and Certain Dangerous Cargoes (CDCs) are accurately tracked and accounted for. Inspectors should question VSOs and other personnel with security duties regarding additional cargo handling security measures for elevations in MARSEC level requirements as specified in their VSP. This includes, but is not limited to, increased screening of cargo and inventory, search of delivery vehicles, vehicle escort provisions, additional measures to prevent tampering (e.g., seals), and suspending operation.*

**21. Security Measures for Delivery of Vessel Stores and Bunkers.**

**33 CFR 104.280**

*Inspectors may observe procedures in place to ensure the security of vessel deliveries and bunkering operations, and whether security personnel show competence in these duties. Inspectors should cite the approved VSP and verify vessel delivery and bunkering procedures for the current MARSEC level are in effect and deemed adequate. These procedures include, but are not limited to, deterrence of tampering with stores, supplies and bunkers, identification of unauthorized deliveries (inventory control), and checking deliveries for dangerous or unauthorized substances. Inspectors should question VSOs and other personnel with security duties regarding additional vessel delivery and bunkering security measures for elevations in MARSEC level requirements as specified in their VSP. This includes, but is not limited to, increased screening of stores and inventory, search of delivery vehicles, vehicle escort provisions, additional measures to prevent tampering (seals), and suspending operations. Inspectors should determine how recurring and non-recurring deliveries are addressed in the VSP.*

**22. Security Measures for Monitoring.**

**33 CFR 104.285**

The VSP may specify a variety of security measures for monitoring. It is generally the practice to conduct vessel inspections during daylight hours, which might determine if some measures are adequate (e.g., lighting). Some measures, such as intrusion, may be tested at any time. In any case, if the inspector is in doubt as to whether a measure is adequate, a demonstration may be necessary.

*The inspector should review the measures that are specified in the VSP and require performance testing of any measure that appears questionable.*

**23. Security Incident Procedures.**

**33 CFR 104.290**

- A. The VSP will have procedures specifying how the VSO and the vessel security personnel will address a security incident at each MARSEC Level. These procedures will detail how the vessel personnel respond to the threat while maintaining critical operation. Items covered vary between vessel but could include 1) prohibiting entry, 2) denying access, 3) stopping operations, 4) notifying authorities, 5) evacuating vessel, and 6) briefing personnel.
- B. In meeting these standards, there is no expectation that vessel personnel be armed in order to repel unauthorized personnel onboard. The requirement to respond to unauthorized personnel onboard a vessel does not necessarily require security personnel to repel unauthorized boarders, but rather to have in place measures that will detect and deter persons from gaining unauthorized access to the vessel. If unauthorized access is attempted or gained at a vessel, then the VSP must describe the security measures to address such an incident, including measures for contacting the appropriate authorities and preventing the unauthorized boarder from gaining access to restricted areas. We are not requiring the owner or operator to put any personnel in “harm’s way,” (i.e., by mandating the use of deadly force to confront deadly force). Security measures for responding to unauthorized personnel will likely be structured on a continuum, depending on the specific threat, which may include confrontation, detention until authorities arrive, or using the force authorized under the appropriate jurisdiction to deal with the threat posed by the unauthorized boarder.

*In verifying compliance with these sections, the individual performing the on-site inspection should confirm that the vessel has the equipment and/or personnel necessary to carryout the procedure as detailed in the VSP. For example, if the plan specifies that, in the event of a security incident, the VSO will notify authorities via radio, does the vessel have a radio that is capable of communicating with the appropriate authorities? Drill should incorporate security incidents procedures that are outlined in the plan.*



**24. Additional Requirements--Passenger Vessels and Ferries.**

**33 CFR 104.292**

- A. Passenger vessels and ferries are required to adhere to higher standards with regard to passenger screening and security sweeps. The regulations offer alternatives to the frequency and extent that such screenings and sweeps are conducted, and the amount of documentation that is required.
- B. A VSP requires a vessel's procedures for monitoring be documented. Although a vessel is not required to record when it conducts a security sweep, some logs may include such details. An inspector should consider whether the security sweep was in accordance with the company's Security Plan, whether the sweep was expanded to cover areas more susceptible based on the port-wide threats (advertised in MARSEC changes), and whether the sweep adhered to the requirements of locally issued MARSEC directives.
- C. When expanding an inspection of this part, a marine inspector should evaluate whether the vessel's security sweeps are adequate. When conducting such an assessment, the inspector should consider the MARSEC level in which the vessel is operating. If the vessel is operating in MARSEC level two or three, the inspector should see additional amounts of compartment and vehicle searches, some of which may be conducted by armed patrols. The inspector should also identify any alternatives that the vessel has implemented, verify that such alternatives are documented in the Security Plan, and ensure that the alternatives are allowable by the regulations. In addition, the inspector should determine whether these alternatives provide an equivalent amount of security for the vessel, i.e., through the combination of searches, patrols, and locking of doors, the vessel is as secure as it would be if it conducted ID checks, screening of passengers and baggage. The inspector should feel confident upon leaving the vessel that the regulations are met and that any alternatives provide that equivalent level of security.

*One important item that the inspector should keep in mind is the fact that the Vessel Security Plans were approved without anyone visiting the vessel. Therefore, if the inspector finds that the alternatives implemented do not provide the equivalent level of security provided by ID checks and screenings, the inspector should require the vessel owner to amend the VSP.*

**25. Additional Requirements--Cruise Ships.**

**33 CFR 104.295**

Unlike the requirements for passenger vessels and ferries, which have various requirements for the amounts of screening, patrolling, and searching, the requirements for cruise vessels are not as flexible. The regulations for this part require screening, ID checks, patrols, and searches to take place.

*An inspector evaluating a cruise ship's adherence to this part of the regulations may conduct the examination in the same manner as they would to determine the compliance of passenger vessels and ferries, i.e., examine specifics of Security Plan, check Official Log or Security Log for vessel's work to accomplish the details of the VSP. When expanding the exam, the inspector may consider background information such as the port's MARSEC level,*

*prevailing MARSEC directives, and port intelligence to determine whether the vessel had adjusted their posture to meet current security threats. An expanded exam could also include accompanying the VSO of the vessel on a patrol, search, or identification check.*

If the inspector finds areas of the plan that is not adequate or, not accurate (based on the configuration of the vessel, i.e., Vessel Security Plan quoted that the vessel did not have a radio room, but an onboard visit to the vessel found otherwise) the plan would need to be amended. Such cases may be common, since these plans were approved without on-site visits.

**26. Additional Requirements--Vessels on International Voyages. 33 CFR 104.297**

The requirements of 33 CFR Part 104 were written to harmonize the requirements of the International Ship and Port Facility Security (ISPS) Code with requirements of 33 CFR 104. Therefore, vessels meeting the requirements of 33 CFR 104 are in compliance with the ISPS Code.

*Prior to undertaking an international voyage, vessels without a current ISSC will need to request an inspection from the local OCMI. After the inspection is completed, and the inspector finds that the provisions of 33 CFR 104 and the ISPS code have been addressed, the vessel will receive an International Ship Security Certificate (ISSC), valid for a maximum of 5 years. An ISSC may not be issued unless a vessel is in full compliance with 33 CFR 104 and the ISPS code i.e., no deficiencies may be issued. An ISSC may be issued for less than 5 years in order that it may harmonize with other International Certificates.*

**27. Assessment . 33 CFR 104.300**

The assessment is a key component of a successful security system. The regulations specify several critical areas that should be addressed by the assessment. The owner or operator may consult an independent expert if needed, as long as these potential vulnerabilities are considered and are either determined not to be a threat or are addressed in the VSP with security measures.

*The inspector should consider whether the measures found in 33 CFR 104.300 (d) have been adequately addressed in the assessment during the verification. If one or more of these considerations do not appear to be addressed, the inspector should discuss it with the VSO or CSO, as appropriate. The inspector may consider asking the name and qualifications of any third party expert consulted during the assessment.*

**28. Vessel Security Plan. 33 CFR 104.400**

33 CFR 104.400(a)(1) requires that the VSP identify of the CSO and VSO by name or position and provide 24-hour contact information.

*Because the CSO is ultimately responsible for the VSP and is usually the direct link to the Coast Guard on all security issues, and because the CSO and their contact information*

*generally change on a relatively infrequent basis, it is preferred that CSO be identified by name in the VSP. Conversely, because VSOs change on a more frequent basis, it is preferred that they be identified in the VSP by title or position only (i.e., Master, Chief Mate, etc.). Identification of the VSO by title or position will eliminate the need for amendment and resubmission of the VSP for Coast Guard approval each time the individual serving as VSO changes. The inspector should ensure that the 24-hour contact information is valid.*

**29. Amendment and Audit.**

**33 CFR 104.415**

- A. Amendments to VSP. The VSPs are living documents, able to change continuously to incorporate changes or lessons learned. Local COTPs may initiate amendments as well as conduct onsite verification of plan changes initiated by the facility/vessel owner or operator. VSP amendments should be tracked and recorded in the vessel file. To ensure amendments are consistent and meet regulatory intent, MSC will review and approve changes to plans. Hence, the regulations dictated specific timeframes for amendments.
- B. Amendments to ASP. Should an enforcement inspection reveal that an owner/operator has correctly implemented an approved ASP in its entirety but security vulnerabilities exist in the vessel operation, the COTP shall be advised. Under 33 CFR 104.415 (a) (ii), the inspector can determine that an amendment is necessary and forward the recommendation through the chain of command to Commandant (CG-543). If deemed appropriate, (CG-543) will advise the organization that submitted the ASP for approval accordingly. Following such notification, it will be necessary for the original submitting organization to provide their proposed amendment to the Commandant (CG-543) for review and approval. If the submitting organization does not wish to amend the ASP, the vessel owner must submit a VSP for the vessel to the MSC. Amendments only include changes that are required or proposed to the plan template.
- C. Audits. At a minimum, the regulations require the CSO or VSO to ensure an annual audit is performed by personnel with knowledge in conducting audits and inspections, and control and monitoring techniques. The use of independent auditors is allowed. Vessels are also given flexibility in how they assign auditors depending on the unique nature and size of the company and vessels. Audits may be required due to structure modifications on the vessel, or changes in operations, security measures, and response plans. Other vessel changes that impact the VSP may also trigger an audit. Audits may result in amendments to the overall VSP.

*Nothing in the regulations prohibits the audit from being performed in conjunction with the scheduled security inspection conducted by the Coast Guard, as long as an audit is done at least once every calendar year. However, the initial audit must be complete not more than one year from the VSP approval date. If a combined inspection/audit is performed, the inspector may review the qualifications of the auditor to ensure that the regulations for auditor's qualifications are met.*

**30. Ship Security Alert System (ISPS Only).**

**ISPS 9.4.18**

Ship Security Alert Systems (SSAS) are a SOLAS XI-2 requirement, and ISPS requires that the VSP include a description of the system. This information is essential in order for the inspector to complete the verification. Enclosure (5) of this NVIC provides guidance on implementing SOLAS XI-2 SSAS requirements to U.S.-flag vessels.

Due to the sensitive security nature of the information, ISPS allows the owner to keep the SSAS information separate from the other parts of the VSP. As described in section 6(B), Enclosure (5) of this NVIC, the details and procedures for an SSAS installed on board a vessel should be contained in a separate annex or supplement to the VSP and stored separately from the Plan to limit access to its details. Access to this annex should be limited to the master, vessel security officer, and other senior personnel designated by the shipping company. .

ISPS also requires the equipment to be installed after the first “survey” of the radio equipment following the deadline. Survey in this case means either the periodical or renewal survey, whichever occurs next after the deadline for compliance. New vessels must have the equipment installed at the initial survey.

*Specifics details will be contained in the VSP describing test procedures for the SSAS. The inspector should follow the test procedures indicated. If the test reveals a problem with either the test procedure or the SSAS itself, the inspector should immediately inform the VSO. The failure of the SSAS represents a serious security deficiency and must be addressed as soon as possible.*

**31. Format of the Vessel Security Plan (VSP).**

**33 CFR 104.405**

33 CFR 104.405(a)(2) requires that the VSP include a section on personnel training. While there are no specific training requirements for CSOs and VSOs, they must meet the corresponding general knowledge qualifications found in 33 CFR 104.210(b) and 33 CFR 104.215(b) respectively. These qualifications may be attained either through formal training or equivalent job experience. 33 CFR 104.405(b) requires that the VSP describe how the qualification requirements will be met.

*The VSP should clearly describe how the company ensures the CSO and VSO meet the qualification requirements, whether by attending a formal course, on-the-job training, or some other acceptable means.*

*The documentation certifying the VSO's qualifications, i.e., course completion certificate, designation letter from a senior company official, etc., should not be included as part of the VSP, however, it should be made available upon request. Maintaining the certifying documentation separate from the approved VSP will eliminate the need for amendment and resubmission of the VSP each time the individual serving as VSO changes.*

*The inspector may verify that the VSP section on personnel training includes general information describing how the company ensures the VSO meets the qualification requirements.*

**ENCLOSURE 4**

**EXCERPTS OF THE PREAMBLE TO THE FINAL RULE**

The information contained herein only addresses the comments that were received to the docket, and, therefore, does not address every issue. However, the responses may be helpful in determining the intent of the regulations.

§ 104.105(a)(1): Non-self propelled Mobile Offshore Drilling Units (MODUs) that meet the threshold characteristics set for OCS facilities will be regulated by 33 CFR part 106, rather than 33 CFR part 104. This is because MODUs act and function more like Outer Continental Shelf (OCS) facilities, have limited interface activities with foreign and U.S. ports, and undergo a higher level of scrutiny for their personnel to obtain visas to work on the OCS.

§ 104.105(a)(6): The intent of the applicability for 33 CFR part 104 was not to include passenger vessels certificated under 46 CFR subchapter K that have overnight accommodations for more than 49 passengers but are not certificated to carry more than 150 passengers; only vessels certificated to carry more than 150 passengers must meet the requirements of 33 CFR part 104.

§ 104.105(a)(7): Small passenger vessels in commercial service regulated under 46 CFR subchapter T and uninspected passenger vessels regulated under 46 CFR subchapter C are not directly regulated in 33 CFR part 104. Small passenger vessels on international voyages do not require a specific waiver, exemption, or endorsement. These vessels will be covered, however, in Area Maritime Security (AMS) Assessments and Plans under 33 CFR part 103. Owners, operators, and others associated with these vessels, including charterers, are encouraged to participate—consistent with § 103.300(b) concerning the AMS Committee charter—in the development of the AMS Plan.

However, vessels making international voyages, which now includes Canadian waters as defined by 33 CFR 101.105 and subject to 46 CFR subchapter T, are required to meet the requirements of 33 CFR part 104. In the past, waivers and equivalencies were granted to some small passenger vessels for some SOLAS safety-related requirements on the basis of their size, passenger capacity, and where they operate. All vessels on international voyages should be subject to 33 CFR parts 104 because of the higher security risks these vessels pose.

§ 104.105(a)(7)(9): There will be vessels on the Great Lakes and St. Lawrence Seaway, which are otherwise exempted from SOLAS that are required to comply with our regulations. Security measures for certain geographic areas, such as the Great Lakes and the St. Lawrence Seaway, are necessary to maintain comparable levels of security throughout the maritime domain. In addition, while SOLAS does not typically apply to the Great Lakes and St. Lawrence Seaway, it allows Contracting Governments to determine appropriate applicability for their national security. For the U.S., the MTSA does not exempt geographic areas from maritime security requirements. If vessel owners or operators believe that any vessel security requirements are unnecessary due to their operating environment, they may apply for a waiver under the procedures allowed in § 104.130. Additionally, vessel owners or operators may submit for approval an Alternative Security Program (ASP) to apply to vessels that operate solely on the Great Lakes and St. Lawrence Seaway.

Under this section, all foreign vessels not carrying an approved International Ship Security Certificate (ISSC) intending to enter a port or place subject to jurisdiction of the U.S.

are required to submit to the Coast Guard a Vessel Security Plan (VSP) prepared in response to the Vessel Security Assessment (VSA), unless they implement an approved ASP. This includes Canadian commercial vessels greater than 100 gross register tons operating solely on the Great Lakes calling at a U.S. port.

§ 104.105(a)(9)(11): It is important to understand that the vessel security requirements were developed to address risks posed by those towing vessels engaged in the transportation of hazardous and dangerous cargoes. These towing vessels and their barges may be involved in a transportation security incident. The focus of the regulations are on towing vessels that transport barges with Certain Dangerous Cargoes (CDC) and barges subject to 46 CFR subchapter D or O, which limits the burden on the towing industry, while increasing maritime security. Even in the case of limited operations, some cargoes are so dangerous that in order to minimize risk, the vessels carrying those cargoes are regulated.

Non-self-propelled vessels (barges) subject to 33 CFR subchapter I must comply with 33 CFR part 104, only if they are carrying CDC in bulk or are engaged on an international voyage.

Towing vessels, such as assist tugs, assist boats, helper boats, bow boats, harbor tugs, ship-docking tugs, and harbor boats, are not subject to 33 CFR part 104 because either the primary towing vessel or the facility will be subject to the regulations and will take such assist vessels into account in the security plan. These vessels typically engage in operations such as docking, undocking, maneuvering, transiting bridges, transiting locks, pulling cuts through a lock, or assisting in an emergency such as a breakaway barge. This exemption is similar to those used in 46 CFR part 27. Owners or operators of towing vessels not directly regulated under 33 CFR part 104 are covered under 33 CFR parts 101 through 103 and, although there are no specific security measures for assistance towing vessels in these parts, the AMS Plan may call for measures that the assisting towing vessels must follow, or the COTP may require security measures to address specific security concerns. Nothing in these regulations alters any duty that a vessel may have to render assistance to those in distress.

104.105(b): Fishing, recreational, and other vessels less than 100 gross tons are not subject to part 104 and are covered by parts 101 through 103 and, although there are no specific security measures for these vessels in these parts, the AMS Plan may set forth measures that will be implemented at the various MARSEC Levels that may apply to them.

If a dredge meets any of the specifications in § 104.105(a), the dredge may be regulated under 33 CFR part 104. For example, if a dredge's operations include towing a tank barge alongside for bunkers, or the dredge engages in an international voyage, the dredge must meet the requirements in 33 CFR part 104. If a dredge does not meet any of the specifications in § 104.105(a), then the dredge is covered by the requirements of 33 CFR parts 101 through 103 and, although there are no specific security measures for dredges in these parts, the AMS Plan may call for measures that the dredge must follow, or the COTP may require security measures to address specific security concerns.

#### § 104.110 Exemptions:

104.110(a): The MTSA exempts certain United States government-owned vessels from the requirement to prepare and submit Vessel Security Plans. However, if a government-owned vessel engages in commercial service or carries even a single passenger for hire, these vessels are subject to regulations. For those certain government-owned vessels exempt from security plans

by the MTSA, the COTP will still work to ensure that security measures appropriate for these vessels' operations are addressed in a manner similar to our current oversight of safety measures. This exemption does not apply to vessels that are leased by or under contract to the United States government.

104.110(b): It will be the under the authority of the cognizant COTP or OCMI to determine if a vessel is truly in lay-up status, dismantled, or out of commission. It is not required that these vessels surrender their certificates. However, it is advisable that using their appropriate authorities (e.g., a COTP Order or CG-835) that the cognizant COPT or OCMI will ensure that the vessel is not returned to service without notification and approval.

§ 104.115 Compliance dates.

§ 104.115(c)(1)(2): Foreign flag vessels need not submit their VSA or VSP to the Coast Guard for review or approval. Owners and operators of foreign flag vessels that meet the applicable requirements of SOLAS Chapter XI will not have to submit their assessments or plans to the Coast Guard for review or approval.

However, some foreign vessels, which may not be subject to or operating under SOLAS, may meet these requirements through either submission to the Coast Guard or their own flag administration. Flag administrations may apply the new international security requirements to vessels other than those required to comply with SOLAS, consistent with paragraph 4.46 of part B of the ISPS Code and Resolution 7 from IMO's Diplomatic Conference on Maritime Security. Furthermore, some flag administrations, not party to SOLAS, may decide to apply SOLAS Chapter XI and the ISPS Code requirements to their vessels trading with the U.S. In these latter two cases—where foreign vessels not subject to SOLAS may nevertheless be required by the flag administration to comply with the requirements of SOLAS Chapter XI and the ISPS Code—the Coast Guard intends to work with the flag administration if they propose initiatives such as an ASP. This will likely be done through bilateral or multilateral arrangements. When no approved ASP or bilateral arrangement exists, foreign flag vessels not subject to SOLAS, but covered by 33 CFR part 104, must submit a VSA and VSP to the Coast Guard for review and approval.

§ 104.120 Compliance documentation.

§ 104.120 (a) (3): The Alternative Security Program (ASP) allows industries, owners or operators of a large numbers of vessel to submit a single generic plan that will cover those vessels.. However, this single generic plan does not alleviate each vessel participating in ASP from conducting a vessel specific security assessment report in accordance with the ASP, and this report must be readily available for Coast Guard inspection.

§ 104.120 (a) (4): Foreign flag vessels required to comply with SOLAS Chapter XI-2 and the ISPS Code are required only to have on board a valid ISSC issued in accordance with section 19 of part A. This includes ensuring that the VSP meets the requirements in SOLAS Chapter XI-2 the ISPS Code, part A, having taken into account the relevant provisions of part B. The ISSC form is contained in Appendix 1 of the ISPS Code, part A. There is no separate requirement in our regulations to document compliance with part B, although flag administrations and RSOs are encouraged to provide such documentation to assist our Port State Control efforts and reduce the potential for vessel delays. This documentation, although



optional, could be in the form of a letter retained on the vessel signed by an authorized representative of the flag administration or RSO that clearly states that the VSP applies the relevant provisions of part B. Part B may be used as one of the tools to assess a foreign vessel's compliance with SOLAS Chapter XI-2 and the ISPS Code, part A. The Coast Guard is using the same cooperative arrangement that was used with success in the safety realm by accepting SOLAS certificates documenting flag state approval of foreign SOLAS VSPs that comply with the comprehensive requirements of the ISPS Code. The consistency of the international and domestic security regimes, to the extent possible, was always a central part of the negotiations for the MTSA and the ISPS Code. In the MTSA, the Congress explicitly found that "it is in the best interests of the U.S. to implement new international instruments that establish" a maritime security system. Port State Control is exercised to ensure that foreign vessels have approved plans and have, in fact, implemented adequate security standards. If vessels do not meet U.S. security requirements, the Coast Guard has, and will not hesitate to use, the power to prevent those vessels from entering the U.S. in appropriate cases. The Port State Control measures will include tracking the performance of all owners, operators, flag administrations, RSOs, charterers, and port facilities. Noncompliance will subject the vessel to a range of control and compliance measures, which could include denial of entry into port or significant delay. The Coast Guard's current Port State Control program has been highly effective in ensuring compliance with SOLAS safety requirements; the incorporation of the ISPS Code requirements into this program is the most efficient and effective means to carry out our Port State Control responsibilities, enhance the ability to identify substandard vessels, ensure the security of our ports, and meet the Congressional intent of the MTSA.

§ 104.120 (b): The inspection regime is designed to verify compliance with the regulations. These inspections may include but are not limited to a port state control exam, an inspection such as for the issuance of a Certificate of Inspection (COI) or an annual re-inspection for endorsement on a COI. For uninspected vessels, inspectors intend to check compliance with these regulations at a frequency that is similar to those of existing uninspected vessel safety programs and in conjunction with other boardings.

§ 104.125 Noncompliance: The intent of this regulation was not to require self-reporting for minor deviations that are corrected immediately. Rather, it is to make it clear that owners or operators are required to request permission from the Coast Guard to continue operations when temporarily unable to comply with the regulations.

§ 104.130 Waivers: Waivers provide flexibility for vessel owners and operators with unique operations. It is important to understand that only Commandant (G-MP) may grant waivers. Waivers will only be issued when there is a compelling reason to do so, and when waivers are intended to be long-term in nature and not for short-term deviations from the regulations.

§ 104.135 Equivalentents: As with waivers, equivalentents provide flexibility for vessel owners and operators dealing with deviations to provide an equivalent level of security with measures not specifically provided for by the regulations. Equivalentencies may be issued by the cognizant COTP and should be limited in duration or limited to their respective COTP zones.

§ 104.200 Owner or operator:

§ 104.200 (b)(6): This regulation requires that the owners or operators of vessels and facilities coordinate shore leave for vessel personnel in advance of a vessel's arrival. However, facilities are not mandated to allow access for shore leave because during periods of heightened security, shore leave may not be in the best interest of the vessel personnel, the facility, and the public. Mandating such access could also infringe on private property rights; however, facility owners and operators are strongly encouraged to maximize opportunities for mariner shore leave and access to the vessel through the facility by seafarer welfare organizations. With regards to visas, the Coast Guard does not issue nor expedite the issuing of visas. Additionally, visas are a matter of immigration law and are beyond the scope of these regulations.

§ 104.210 Company Security Officer (CSO):

§104.210(a)(3): This section and § 104.215(a)(1) does not preclude an owner or operator of a company that owns vessels from appointing the same individual as both the Company Security Officer (CSO) and Vessel Security Officer (VSO). The CSO may also be the VSO, provided he or she is also able to perform the duties and responsibilities required of both positions. Generally, this provision is for vessels operating on restricted routes in a single COTP zone and for unmanned vessels. Under § 104.215(a)(2), however, the VSO for manned vessels must be the Master or a member of the crew.

104.210(a)(4): This regulation provides flexibility for a Company Officer to assign security duties to other vessel personnel. The CSO may delegate duties required in 33 CFR part 104, including conducting Vessel Security Assessments (VSAs). The CSO remains responsible for the performance of all security-related duties, even when delegated. Under § 104.300(c), third parties may work on a VSA so long as the CSO reviews and accepts their work. An owner or operator is also allowed to designate more than one Company Officer. Because the CSO's responsibilities are key to security implementation, vessel owners and operators are encouraged to assign an alternate CSO to coordinate vessel security in the absence of the primary CSO.

§ 104.215 Vessel Security Officer (VSO):

§ 104.215(a)(3) Vessel Security Officers (VSOs) are required on towing vessels greater than 8 meters engaged in towing barges that transport hazardous or dangerous cargos; it is imperative that the responsibility for security on these vessels be clearly established. Recognizing that some of these towing vessels will have a small crew complement, the Master is not prohibited from being the VSO. Section 104.200 provides that the VSO can be designated by name or by title. The duties of the VSO ensure that a knowledgeable person is on board or is directly responsible for coordinating the implementation of the Vessel Security Plan. It is not the

intention of the regulations to preclude a CSO from also serving as a VSO for a towing or unmanned vessel.

§ 104.215(a)(5) An owner or operator is allowed to designate more than one VSO. Because a VSO's responsibilities are key to security implementation vessel owners and operators are encouraged to assign an alternate VSO to coordinate vessel or facility security in the absence of the primary VSO.

§ 104.215(b): The intent of this section is to outline those responsibilities that are necessary for all VSOs to effectively implement the security measures contained in Vessel Security Plans. However, this section provides the maximum flexibility to the VSOs by allowing them to assign security duties to other crewmembers so long as the security of the vessel's operations is not compromised. In this way, other crewmembers can assist the VSO and learn about security related duties. Additionally, these people may acquire general knowledge through training or equivalent job experience.

§ 104.225 Security training for all other vessel personnel: These requirements are meant to be basic security and emergency procedure training requirements for all personnel. In most cases, the requirement is similar to the basic safety training given to visitors of a facility to ensure that they do not enter areas that could be harmful. To reduce the burden of these general training requirements, vessel and facility owners and operators are allowed to recognize equivalent job experience in meeting this requirement. However, contractors need basic security training as much as any other personnel working on the vessel or facility. Providing basic security training (e.g., how and when to report information, to whom to report unusual behaviors, how to react during an emergency) could be sufficient depending on the vessel or facility. To emphasize this, § 104.225 allows the owners or operators of vessels and facilities to determine which basic security training requirements are appropriate for their operations.

§ 104.230 Drill and exercise requirements:

§ 104.230 (b)(2): The nature of unmanned barges precludes the intensive personnel drills required for testing proficiency. However, each vessel subject to 33 CFR parts 104, whether manned or unmanned, is required to submit a Vessel Security Plan for approval that includes drill and exercise requirements. Under § 104.230(b)(2), this plan should include those drilling requirements that are appropriate for the nature and scope of that vessel's activity, and adequately prepare the VSO to respond to those threats the vessel is most likely to encounter.

§ 104.230(b)(4): It could be difficult to conduct drills for companies that rotate crews frequently or have standing relief crews. Therefore this regulation was written to allow companies that operate vessels of similar design not subject to SOLAS to develop training and drill schedules that are more appropriate to their operations while keeping the standard of 25 percent. For example, a company operating several similar towing vessels could hire new crewmembers, have them participate in a drill on board one towing vessel, then rotate those crewmembers to any of the similar vessels within that same company's fleet. Finally, we added the word "from" between "week" and "whenever" in § 104.230(b)(4) and (5) for clarity.

§ 104.230(c)(2)(iii): Exercising the Vessel Security Plan (VSP) frequently is essential to ensure the plan is effectively implemented; therefore, there is an annual requirement for an exercise of the VSP. Recognizing that participation in exercises can be time consuming and challenging to coordinate, the regulations allowed and encourage vessel owners and operators to combine security exercises with other exercises as stated in § 104.230(c)(2)(iii).

§ 104.235 Vessel recordkeeping requirements:

§104.235(a): Records must be made available to the Coast Guard upon request, and §§ 104.235(c) states that the record must be protected from unauthorized access. This section does not mandate, nor preclude the records from being stored some place other than the vessel. In the case of some types of vessels (e.g., towing vessels, unmanned barges) it would be impractical to maintain such records on board and for those vessels that make only domestic voyages. With the exception of Declarations of Security (DoS), these records may be kept somewhere other than on board the vessel, so long as they can be made available to the Coast Guard expeditiously upon request. However, vessel owners and operators must recognized that if they choose to store these records some place other than the vessel, their vessels may be delayed while they retrieve the records for Coast Guard inspection. For vessels subject to SOLAS and the ISPS Code (part A), section 10 requires records to be kept on board.

§§ 104.235(b)(1): The intent of this regulation was not to record all training but only training required under § 104.225 is to be reported.

§ 104.235(b)(7): This section requires that manned vessels must keep on board a copy of the last 10 Declarations of Security (DoS) and a copy of each continuing DoS for at least 90 days after the end of its effective period. The regulations require both vessels and facilities to retain the DoS for their last 10 port visits even after expiration. . In order to roughly align the facility's retention requirement, a 90-day retention period would more closely align with the vessel's 10-port visit retention period rather than the 30-day period used for declarations of inspection. Many factors, such as not being within U.S. waters during MARSEC Levels 2 and 3, may delay a vessel's ability to accumulate 10 DoS's. If a vessel has on board fewer than the number of DoS's required as stated in § 104.235(b)(7), it is acceptable for the vessel to continue operating as long as it plans to meet the intent of the section by verifying that it was not required to keep on board more than the number of DoS completed.

§ 104.240 Maritime Security (MARSEC) Level coordination and implementation:

§ 104.240(b)(2) This section does apply to unmanned vessel because regulations allow for a VSO to be a company representative for unmanned vessels; the VSO may be designated by the owner or operator to provide reports on the attainment of increased MARSEC Levels to the appropriate COTP as specified in § 104.240. Any vessel, manned or unmanned, must be under the cognizance of a VSO or a CSO to ensure security measures are properly implemented.

§ 104.240(c): The intent of the requirement is to disclose as much information available and appropriate to vessel personnel to mitigate risk even if a threat is not identified. If there is no identified threat, the VSO is still required to brief all vessel personnel, emphasizing reporting procedures and the need for increased vigilance.

§ 104.240(e)(1)(2)(3): Owners and operators have the authority to implement the security measures for MARSEC Level 3, which include armed patrols, waterborne security, and underwater screening. For example, it is well settled under the law of every State that employers may maintain private security guards or private security police to protect their property. The regulations do not require owners or operators to undertake law enforcement action, but rather to implement security measures consistent with their longstanding responsibility to ensure the security of their vessels and facilities as specifically prescribed by 33 CFR 6.16-3 and 33 CFR 6.19-1, by deterring transportation security incidents; detecting an actual or a threatened transportation security incident for reporting to appropriate authorities; and, as authorized by the relevant jurisdiction, defending themselves and others against attack. It is also important to note that the security measures listed in §§ 104.240(e) and 105.230(e) are not exclusive and only relate to MARSEC Level 3 implementation. In many instances, the owner or operator may decide to implement these security measures through qualified contractors or third parties who can provide any expertise that is lacking within the owner's or operator's own organization with the required authority.

Further, the intent of these regulations is not to mandate the use of crewmembers to perform waterside security, although that is an option. Those vessel owners and operators choosing to implement waterside security to meet the requirement of § 104.265(f) to ensure access control through additional measures during MARSEC Level 2, and to enhance the security of the vessel during MARSEC Level 3, may choose to enter into agreements with the facility owner or operator, private security firms, or other parties.

Vessel owners and operators are not exempt from any existing work hour and rest requirements, such as STCW and International Labor Organization requirements, when implementing security requirements at higher MARSEC Levels. The VSP must address how the security measures will be implemented at each MARSEC Level. Manning concerns must be considered during the VSP development and addressed in implementation.

§ 104.255 Declaration of Security (DoS): The fundamental intent of these regulations is to establish cooperation and communication between facilities and vessels to minimize the potential for a transportation security incident. A facility that places the onus on vessels to provide all the security would be acting contrary to the regulations. When approving security plans, the COTP has the discretion to determine whether a facility has implemented sufficient security measures to meet the requirements of these regulations. Any agreements or mandates that the facility owner or operator intends to prescribe to vessels should be reflected in the Facility Security Plan.

§ 104.255(a): As specified in § 101.505, the format of a DOS is described in SOLAS Chapter XI-2, Regulation 10, and the ISPS Code. The timing requirements for the are specified §§ 104.255 and 105.245. The format for a can be found as an appendix to the ISPS Code.

§ 104.255: In § 104.205(b), if in the professional judgment of the Master, a conflict between any safety and security requirements applicable to the vessel arises during its operations (e.g., adverse weather), the Master may give precedence to measures intended to maintain the safety of the vessel and take such temporary security measures as deemed best under all circumstances. Therefore, if the DoS between a vessel and facility could not be safely exchanged, the Master would not need to exchange it before the interface. However, under § 104.205(b)(1), (b)(2), and (b)(3), the Master would have to inform the nearest COTP of the

delay in exchanging it, meet alternative security measures considered commensurate with the prevailing MARSEC Level, and ensure that the COTP was satisfied with the ultimate resolution.

To maintain flexibility, the regulations neither preclude nor mandate a specific means for communicating about a DoS, as long as either parties or the designees sign the DoS prior the vessel-to-vessel or vessel-to-facility interface. Vessel-to-vessel activity in the Exclusive Economic Zone is not included in these regulations. However, these regulations do apply to vessels interfacing with OCS facilities regulated under 33 CFR part 106.

§ 104.255 (e)(2)(3): Continuing Declaration of Security (DoS) Declaration of Security (DoS) agreements among vessel and facility owners and operators should be periodically reviewed in response to the frequent change in operations, personnel, and other conditions. The DoS ensures essential security-related coordination and communication between vessels and facilities. Renewing a continuing DoS agreement only requires a brief interaction between vessel and facility owners and operators to review the essential elements of the agreement. Additionally, at a heightened level of threat, that change in threat must be assessed, and a new DoS must be completed. Less frequent reviews, such as during an annual or biannual review of the Vessel Security Plan, does not provide adequate oversight of the DoS agreement to ensure all parties are aware of their security responsibilities.

Unmanned barges are not required to complete a DoS at any MARSEC Level.

§ 104.265 Security measures for access control: The owner or operator must ensure the implementation of security measures to control access because unmanned barges directly regulated under this subchapter may be involved in a transportation security incident. As provided in § 104.215(a)(4), the Vessel Security Officer (VSO) of an unmanned barge must coordinate with the VSO of any towing vessel and Facility Security Officer of any facility to ensure the implementation of security measures for the unmanned barge.

§ 104.265 (e)(1): Screening of persons, their personal effects, and vehicles are necessary at all MARSEC Levels to minimize the risk of a transportation security incident. However, while all vessels must implement screening procedures, the flexibility in determining those screening procedures should consider the vessel type and the geographical region it is operating. Additionally, the intent of the regulations is that the secure area used to conduct the screening of baggage or personal effects could be the same location of the screening of persons entering the vessel. The screening requirements in the final rules retain the provisions for designating a secure area on board or in liaison with the facility for conducting inspections and screening.

Additionally, while the regulations require vessel owners and operators to deter the introduction of dangerous substances and devices. The regulations do not mandate checking for lawfully carried firearms. The regulations are flexible enough to handle daily operations and allow the owners and operators to develop appropriate procedures to ensure the security of its passenger or commercial activities. All security plans will be reviewed by the Coast Guard to ensure compliance with access control regulations.

§ 104.265 (e)(3): The effectiveness and constitutionality of this section that requires identification checks of passengers and workers are serious concerns. Identification checks, by themselves, may not ensure effective access control, but they can be critically important in attaining access control. The regulations implement the MTSA and the ISPS Code by requiring vessel and facility owners and operators to include access control measures in their security

plans. However, instead of mandating uniform national measures, owners and operators are free to choose their own access control measures. In addition, the rules contain several provisions that work in favor of privacy. Identification systems must use disciplinary measures to discourage abuse. Owners and operators can take advantage of rules allowing for the use of alternatives, equivalents, and waivers. Passenger and ferry vessel owners are specifically authorized to develop alternatives to passenger identification checks and screening. Signage requirements ensure that passengers and workers will have advance notice of their liability for screening or inspection. Vessel owners and operators are required to give particular consideration to the convenience, comfort, and personal privacy of vessel personnel. Taken as a whole, these rules strike the proper balance between implementing the MTSA's provisions for deterring transportation security incidents and preserving constitutional rights to privacy, travel, and association.

§ 104.265(e)(9): This section ensures that the owner or operator of a vessel does not abuse these regulations by regularly requiring crewmembers to screen other crewmembers. There maybe times when it is appropriate, but these time should be few and conducted in a way that takes into full account the individual's human rights and preserves the individual's basic human dignity.

§ 104.265(e)(15): The regulatory language in this section does not require vessel personnel be armed in order to repel unauthorized personnel onboard, although it is an option. The requirement to respond to unauthorized personnel onboard a vessel does not necessarily require security personnel to repel unauthorized boarders, but rather to have in place measures that will detect and deter persons from gaining unauthorized access to the vessel or facility. If unauthorized access is attempted or gained at a vessel or facility, then the Vessel Security Plan or Facility Security Plan must describe the security measures to address such an incident, including measures for contacting the appropriate authorities and preventing the unauthorized boarder from gaining access to restricted areas. The regulations do not require the owner or operator to put any personnel in "harm's way," (i.e., by mandating the use of deadly force to confront deadly force). Security measures for responding to unauthorized personnel will likely be structured on a continuum, depending on the specific threat, to include confrontation, detention until authorities arrive, or using the force authorized under the appropriate jurisdiction to deal with the threat posed by the unauthorized boarder. Owners and operators may find guidance in the IMO's Circular titled "Piracy and Armed Robbery: Guidance to ship owners and ship operators, shipmasters and crews on preventing and suppressing acts of piracy and armed robbery against ships," MSC/Cir.623/Rev.3, to be a useful reference in this regard.

§ 104.270 Security measures for restricted areas:

§ 104.270(b): While the word "must" in this section requires owners or operators to designate restricted areas, the word "appropriate" allows flexibility for owners or operators to restrict limited areas that are significant to their operations.

§ 104.270(d): This section provides a non-exhaustive list of security measures that an owner or operator may use to prevent unauthorized access to restricted areas. Only one of these measures addresses the locking or securing of access points to restricted areas. Other methods include monitoring, using guards, or using automatic intrusion detection. The owner or operator

may also use other measures to prevent unauthorized access. The potential competition between maximizing safety and maximizing security in § 104.205(b) state that “If... a conflict between any safety and security requirements applicable to the vessel arises during its operations, the Master may give precedence to measures intended to maintain the safety of the vessel, and take such temporary security measures as seem best under all circumstances.” However, this provision does not circumvent overall security of the vessels because the section also requires, in § 104.205(b)(3), that the owner or operator ensure the conflict is permanently resolved to the satisfaction of the Coast Guard.

§ 104.275 Security measures for handling cargo: Screening for dangerous substances and devices is a complex and technically difficult task to implement. Cargo checks should be focused on the cargo containers or other cargo transport units arriving at or on the facility or vessel to detect evidence of tampering. These checks are also to prevent cargo that is not meant for carriage from being accepted and stored at the facility without the knowing consent of the facility owner or operator. The issue of cargo screening will be addressed by TSA, BCBP, and other appropriate agencies through programs such as the Customs-Trade Partnership Against Terrorism (C-TPAT), the Container Security Initiative (CSI), performance standards developed under section 111 of the MTSA, and the Secure Systems of Transportation (SST) under 46 U.S.C. 70116. The requirement to ensure the coordination of security measures with the shipper or other party aligns with the ISPS Code. It is intended that provisions be coordinated when there are regular or repeated cargo operations with the same shipper. This coordination facilitates security between the shipper and the facility; therefore, this type of coordination mandatory.

§ 104.275(b)(1): This section emphasizes that a check on cargo and cargo spaces should be done unless it is unsafe to do so.

§ 104.275(b)(4): This section requires the check of seals or other methods used to prevent tampering. This check should primarily be conducted by the facility prior to loading, but it is the responsibility of the vessels to liaise with the facility to ensure that it is done.

§ 104.285 Security measures for monitoring.

§ 104.285(a)(1): As discussed above, it is the vessel owner or operator’s responsibility to ensure that manning levels are sufficient to implement the approved VSP at all MARSEC Levels. There are various ways to meet this requirement, including not operating at higher MARSEC Levels or limiting vessel operational hours to ensure crew rest periods are maintained.

§ 104.290 Security incident procedures.

Section 104.290(a): This section requires vessel owners or operators to ensure that the Vessel Security Officer and vessel security personnel can respond to threats and breaches of security and maintain “critical vessel and vessel-to-facility interface operations,” while paragraph (e) of that section requires non-critical operations to be secured in order to focus a response on critical operations. The Coast Guard does not define the critical operations that need to be maintained during security incidents, because these will vary depending on a vessel’s physical and operational characteristics but requires each vessel to provide its own definition as part of its VSP. Section 104.305(d) requires that they discuss and evaluate in the Vessel Security



Assessment report key vessel measures and operations, including operations involving other vessels or facilities.

§ 104.297 Additional requirements--vessels on international voyages.

§ 104.297(c): This section does not preclude a vessel from being inspected in a place other than a port. It is common industry practice for some inspections to take place in locations other than ports; the language in this section alters that practice.

104.305 Vessel Security Assessment (VSA) requirements.

§ 104.305(d)(2): The owner or operator is responsible for the Vessel Security Assessment but may have a naval architect or other qualified professional evaluate the structural integrity of the vessel in conducting the assessment.

§ 104.310 Submission requirements.

§ 104.310(a): The security assessment reports must be submitted as part of the security plan approval process to determine if they adequately address the security requirements of the regulations.

§ 104.400 Vessel Security Plan (VSP), General.

§ 104.400(c): Security plans are sensitive security information that must be protected in accordance with 49 CFR part 1520. Only those persons specified in 49 CFR part 1520 will be given access to security plans. Also in accordance with 49 CFR part 1520 and pursuant to 5 U.S.C. 552(b)(3), sensitive security information is exempt from disclosure under the Freedom of Information Act (FOIA). However, §§ 104.220 part 104.225 of these rules state that vessel personnel must have knowledge of relevant provisions of the security plan. Therefore, vessel owners or operators will determine which provisions of the security plans are accessible to crewmembers and other personnel. Information designated as sensitive security information is generally exempt under FOIA, and State disclosure laws that conflict with 49 CFR part 1520 are preempted by that regulation. 46 U.S.C. 70103(d) also provides that the information developed under this regulation is not required to be disclosed to the public.

§ 104.405 Format of the Vessel Security Plan (VSP).

§ 104.405(a): In the development of a VSP, it should be understood that nothing in these regulations requires vessel owners or operators to contract for such services in advance. However, if an owner or operator of a vessel develops and has approved a VSP that states it will hire shore-based companies to provide certain security measures, then the vessel owner or operator must be prepared to demonstrate that the plan can be implemented as approved. It is the intent of these regulations that vessel owners or operators, in accordance with their Vessel Security Assessments, identify those resources they will need at the various MARSEC Levels to ensure that they can implement their VSP.

§ 104.410 Submission and approval.

§ 104.410 (a)(1): While the regulations requires the VSP be submitted in English, owners or operators of a vessel are encouraged to provide a translation in the working language of the crew to ensure that vessel personnel can perform their security duties. Additionally, to meet our international obligations, foreign vessels are not required to carry on board the vessel a

copy of its VSP written in English, but it would help Port State Control efforts if the plan were maintained in English as well. Part A of the ISPS Code permits VSPs to be written in the working language or languages of the ship, so long as a translation of the plan is provided in English, Spanish, or French. As stated in the preamble of the temporary interim rule (68 FR 39297), a vessel may be delayed while translator services are acquired when a Port State Control officer is presented a VSP in a language that he or she does not understand.

Index

<b>Term</b>	<b>Page</b>	<b>Section</b>
Additional requirements, vessels on international voyages	12	104.285(a)(1)
Alternative Security Program (ASP), Great Lakes	13	104.297
Alternative Security Program (ASP), purpose	2	104.105(a)(7)(9)
Area Maritime Security (AMS) Assessments and Plans	4	104.120(a)(3)
Barges, Certain Dangerous Cargoes (CDC)	2	104.105(a)(7)
Barges, drills and exercises	3	104.105(a)(9)(11)
Barges, Subchapter I	7	104.230 (b)(2)
Barges, unmanned, MARSEC levels	3	104.105(a)(9)(11)
Barges, Vessel Security Plan	8	104.240(b)(2)
Canadian commercial vessels	7	104.230 (b)(2)
Canadian waters	2	104.105(a)(7)(9)
Certain Dangerous Cargoes (CDC), barges	2	104.105(a)(7)
Certificate of Inspection (COI)	3	104.105(a)(9)(11)
Compliance dates	5	104.120 (b)
Compliance documentation, discussed	4	104.115
Critical vessel and vessel-to-facility interface operations	4	104.120
CSO - Company Security Officer	12	104.290(a)
CSO, also serving as VSO	6	104.210
CSO, delegation of duties	6	104.210(a)(3)
Declaration of Security (DoS), at OCS facilities	6	104.210(a)(4)
Declaration of Security (DoS), continuing	9	104.205(b)
Declaration of Security (DoS), discussion	10	104.255 (e)(2)(3)
Declaration of Security (DoS), unsafe situations	9	104.255
Declaration of Security (DoS), recordkeeping	10	104.205(b)
Declaration of Security (DoS), retention	8	104.235(a)
Dredges	8	104.235(b)(7)
Drill and exercise, rotating crews	3	104.105(b)
Drill and exercise, unmanned barges	7	104.230(b)(4)
English language requirement, VSP	7	104.230 (b)(2)
Equivalentents, discussed	13	104.410 (a)(1)
Exemptions	6	104.135
Fishing vessels	3	104.110(a)
Foreign flag vessels, Part B of ISPS Code	3	104.105(b)
Foreign flag vessels, submission of plans	4	104.120(a)(4)
Government-owned vessels	4	104.115(c)(1)(2)
Great Lakes	3	104.110(a)

Enclosure (4) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 04 03

<b>Term</b>	<b>Page</b>	<b>Section</b>
International Ship Security Certificate (ISSC)	2	104.105(a)(7)(9)
ISPS Code vessels	2	104.105(a)(7)(9)
ISPS Code, part A & B	4	104.115(c)(1)(2)
Laid-up vessels	4	104.120(a)(4)
Manning levels, security measures for monitoring	4	104.110(b)
Maritime Security (MARSEC) Level coordination	8	104.24
MARSEC levels, crew orientation	9	104.240(e)(1)(2)(3)
MARSEC levels, security guards	8	104.240(c)
MARSEC levels, unmanned barges	8	104.240(b)(2)
Mobile Offshore Drilling Units (MODU)	2	104.105(a)(1)
Noncompliance, discussed	5	104.125
Other vessels < 100 GT	3	104.105(b)
Overnight accommodations	2	104.105(a)(6)
Owner or operator, discussed	6	104.200
Recordkeeping requirements	8	104.235(a)
Recreational vessels	3	104.105(b)
Safety and security, conflicts	12	104.270(d)
Security guards, MARSEC levels	9	104.240(e)(1)(2)(3)
Security incident procedures	12	104.290(a)
Security measures for access control, crew screening	11	104.265(e)(9)
Security measures for access control, discussion	10	104.265
Security measures for access control, ID checks	10	104.265 (e)(3)
Security measures for access control, screening	10	104.265 (e)(1)
Security measures for access control, security guards	11	104.265(e)(15)
Security measures for handling cargo	12	104.275
Security measures for handling cargo, checks	12	104.275(b)(1)
Security measures for handling cargo, coordination	12	104.275
Security measures for handling cargo, seals	12	104.275(b)(4)
Security measures for monitoring, manning levels	12	104.285(a)(1)
Security measures for restricted areas, methods	11	104.270(d)
Security training for all other vessel personnel	7	104.225
Shore leave	6	104.200 (b)(6)
SOLAS, Great Lakes Applicability	2	104.105(a)(7)(9)
SSI - sensitive security information, VSP	13	104.400(c)
St. Lawrence Seaway	2	104.105(a)(7)(9)
Subchapter C vessels	2	104.105(a)(7)
Subchapter I barges	3	104.105(a)(9)(11)
Subchapter K vessels	2	104.105(a)(7)

Enclosure (4) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 04 03

<b>Term</b>	<b>Page</b>	<b>Section</b>
Submission and approval, VSP	13	104.410 (a)(1)
Submission requirements, VSA reports	13	104.310(a)
UTV, assist	3	104.105(a)(9)(11)
UTV, requirement for a VSO	6	104.215(a)(3)
Verification exam	5	104.120 (b)
Vessel Security Assessment (VSA) requirements	13	104.305
Vessel Security Assessments (VSAs), conducting	6	104.210(a)(4)
Vessel Security Plan, barges	7	104.230 (b)(2)
Vessel Security Plan, exercising	8	104.230(c)(2)(iii)
Vessels on international voyages, additional requirements	13	104.297
VSA reports, submission requirements	13	104.310(a)
VSO - Vessel Security Officers	6	104.215(a)(3)
VSO, also serving as CSO	6	104.210(a)(3)
VSO, multiple	7	104.215(a)(5)
VSO, responsibilities	7	104.215(b)
VSO, training	7	104.215(b)
VSP, format	13	104.405(a)
VSP, SSI - sensitive security information	13	104.400(c)
VSP, Submission and approval	13	104.410 (a)(1)
Waivers, discussed	6	104.130

Enclosure (5) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 04-03

**ENCLOSURE 5**

**SHIP SECURITY ALERT SYSTEMS**

ENCLOSURE 5  
SHIP SECURITY ALERT SYSTEMS

1. Introduction:

- A. This enclosure provides guidance on implementing the International Convention for the Safety of Life at Sea (SOLAS), Regulation XI-2/6 as it applies to U.S.-flag vessels. It is intended to provide information for U.S. Coast Guard field offices, vessel owners and operators, and others involved with ship security alerting, as well as provide guidelines for developing systems to meet the requirements of SOLAS, Regulation XI-2/6.
- B. U.S. Coast Guard marine inspectors should review the guidance contained in this section to determine if a ship security alert system (SSAS) installed on an U.S.-flag vessel is suitable for its intended purpose, and that it is in compliance with the requirements of SOLAS, Regulation XI-2/6.
- C. SSAS has been developed to provide a vessel master or operator the ability to send a covert alert to shore regarding a security threat to the vessel. SOLAS, Regulation XI-2/6, which requires the fitting of SSASs on certain SOLAS certified vessels, was adopted in December 2002 in conjunction with the International Ship and Port Facility Security (ISPS) Code. Performance standards for the SSAS were adopted by the International Maritime Organization (IMO) in MSC Resolution MSC.147 (77). This document is available at the following address:  
[http://www.navcen.uscg.gov/marcomms/imo/msc\\_resolutions/default.htm](http://www.navcen.uscg.gov/marcomms/imo/msc_resolutions/default.htm).
- D. SSAS alerts originate aboard the threatened ship, and are transmitted by communications service providers (that provide mobile satellite, terrestrial radio, or ground links) to competent authorities designated by the vessel's flag state, and are relayed to the flag state. The flag state is then responsible for notifying appropriate authorities of coastal states in the vicinity of the ship or other states as appropriate.
- E. SSASs are one-way, ship-to-shore alerting systems for situations where lives may be in grave and imminent danger. Therefore, it is essential that the SSAS on board vessels, satellite links, land earth stations, ground communications, and other elements used in transmitting or relaying security alerts to competent authorities ashore be fast, function properly, and be highly available and reliable. These alerts are not "distress alerts" covered by separate requirements of IMO and the International Telecommunications Union, but are comparable and intended to address equally dangerous shipboard situations. Since the SSAS is comparable to equipment used to provide distress alerts to search and rescue authorities, the SSAS and its associated satellite and shore systems should meet comparable standards.
- F. Ships have various communications channels or methods available to help deal with acts of violence that pose security threats to ships, and are used for alerting, assisting with the response, resolving inadvertent alerts, and submitting follow up reports. In the event of an

actual, developing, or apparent security threat, or when the security of the ship has actually been compromised, SSASs are not the only allowable means of alerting the Administration or Competent Authority of security threats to vessels. If suspected attacks are detected early, or if suitable opportunities arise that would not further endanger persons onboard, other means of communications may be used.

2. Definitions: The following terms and definitions relate to security threats and alerting terminology:

*Activation*: The human intervention aboard the ship that sets in motion the automated alert system.

*Acts of Violence*: Acts of terrorism and violent acts that threaten the vessel's security, piracy, acts of armed robbery against ships, and any other security incidents directed against a ship, where the term "ship" is understood to include all persons on board.

*Communications Service Provider (CSP)*: An entity responsible for all or part of the delivery of security alert messages from ships to recognized Administrations, competent authorities, or Tracking Service Providers (TSP).

*Competent Authority*: Designated authority that receives SSAS alerts from ships and informs the appropriate Administration. See Paragraph 5 of this document for guidance regarding competent authorities.

*Priority Access*: Treatment given by communications systems to place distress and ship security alerts and calls ahead of all other traffic.

*Satellite System*: The space segment, land earth station (or equivalent), and arrangements for controlling the space segment and the network control facilities governing access.

*Ship Security Alert System (SSAS)*: Shipboard system required by SOLAS Regulation XI-2/6 to covertly send an alert to a competent authority of a vessel's flag state indicating a security threat to the vessel.

*Test Mode*: Resetting, delaying or preventing the transmission of an alert for the purposes of testing during inspections.

*Tracking Service Provider (TSP)*: An entity that is responsible for all or part of the delivery of security alert messages from either ships or CSPs to competent authorities.

*Transmission Termination*: The human intervention aboard the ship that legitimately stops the automated alert system. This could include keying in a combination or password or pushing a button. Termination can't be done from the activation device and does not cancel the alert.



3. Compliance Dates: The following SOLAS vessels are required to install SSAS equipment:
  - A. Ships constructed on or after 1 July 2004;
  - B. Passenger ships, including high-speed passenger crafts, constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004;
  - C. Oil tankers, chemical tankers, gas carriers, bulk carriers and cargo high speed crafts, of 500 gross tonnage and upwards constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2004; and
  - D. Other cargo ships of 500 gross tonnage and upward, and Mobile Offshore Drilling Units (MODUs) constructed before 1 July 2004, not later than the first survey of the radio installation after 1 July 2006.
4. Voluntary Compliance: SSASs may also be voluntarily installed aboard other vessels. Such installations should generally comply with the requirements of this Circular, particularly with regard to SSAS approval, registration, and testing.
5. Competent Authority:
  - A. SOLAS XI-2/6 allows the Administration to designate a competent authority to receive alert signals from vessels. The Coast Guard, acting as the Flag Administration, has chosen to retain the responsibility of receiving alert messages. Specifically, Rescue Coordination Center (RCC) Alameda, a Coast Guard unit equipped to handle such duties, is the only U.S. entity authorized to receive such alerts. RCC Alameda will work closely with Headquarters and Operational Commanders to relay all alert information. This information will be used to coordinate response protocol for vessels operating within U.S. waters and those operating abroad. No other competent authorities will be designated by the United States for the purposes of receiving SSAS alerts.
  - B. Contact information for RCC Alameda is as follows:

Address: Commander, U.S. Coast Guard  
Attn: RCC Alameda  
Coast Guard Island  
Alameda, CA 94501

Voice: (510) 437-3701  
Fax: (510) 437-3017  
Telex: 230172343  
E-mail: [ssas@uscg.mil](mailto:ssas@uscg.mil)

- C. Voice reports of an alert are preferred. While email and fax reports are acceptable under international protocol, it is recommended that such reports are followed up by a phone call. The follow-up phone call is critical, as it provides RCC Alameda an immediate point of contact to assist in the validation of the ship security alert.
  - D. It should be noted that the National Response Center (NRC), a clearinghouse for most maritime emergency notifications, should NOT be contacted for a ship security alert, and is not set up to receive reports of a ship security alert.
  - E. RCC Alameda, as the recipient of the SSAS alerts, will also be the primary agency documenting the reports in accordance with the Marine Information for Safety and Law Enforcement (MISLE) SSAS Alert Documentation Guide available at:  
<http://mislenet.osc.uscg.mil/>.
6. Submission of System Details for Approval:
- A. The U.S. Coast Guard will not complete a formal type approval for SSASs. Each SSAS will be evaluated for compliance with the performance standards in MSC.147 (77), the technical requirements of this NVIC and, as applicable, as part of the Security Plan approved for the vessel. Companies or organizations desiring to provide SSAS services for U.S. vessels may provide the U.S. Coast Guard with a detailed description of the equipment to be installed or modified. Companies or organizations wishing to act as Communications Service Providers (CSPs) may provide details of their capabilities to monitor and forward alerts to the U.S. Coast Guard. This information should be submitted to Commandant (CG-3PSE-3) for review at the following address:  
  
Address: Commandant (CG-3PSE-3)  
2100 Second Street, SW  
Washington, DC 20593-0001  
Voice: (202) 372-1378  
Fax: (202) 372-1925
  - B. Vessel specific details of each SSAS will be reviewed and approved by the U.S. Coast Guard Marine Safety Center (MSC). For security purposes, the details and procedures for an SSAS installed on board a vessel should be contained in a separate annex or supplement to the vessel's security plan and stored separately from the plan to limit access to its details. Access to this annex should be limited to the master, vessel security officer, and other senior personnel designated by the shipping company. The SSAS information does not need to be submitted to the MSC until required according to the implementation schedule. The majority of U.S.-flag SOLAS vessels will likely submit their SSAS information to MSC after the U.S. Coast Guard has already approved their security plan. If a vessel has a previously approved plan, only the annex covering the SSAS needs to be submitted for review. MSC's address for visitors and courier service is the following:

Address: Commanding Officer (MSC)  
USCG Marine Safety Safety Center  
Jemal Riverside Building  
1900 Half Street SW, Suite 1000, RM 525  
Washington, DC 20024

Voice: (202) 475-3444

Fax: (202) 475-3920

7. Installation of SSAS on board SOLAS Vessels: U.S. Coast Guard Officers in Charge, Marine Inspection (OCMIs) will verify the correct operation of all SSASs installed on board U.S. vessels subject to SOLAS Regulation XI-2/6, and verify the SSAS installation complies with the system described in the approved Vessel Security Plan.
8. System Requirements:
  - A. SSASs should comply with the provisions of MSC.147 (77) on performance standards for ship security alert systems. The transmission of a security alert should not be included with any other routine reporting that the ship may conduct. The activation of a security alert should only require a single action to exclude the opening of protective covers. There must be at least two activation points: one must be located on the navigation bridge and at least one other in an area where it would normally be immediately accessible (e.g., engine room control, master's stateroom, crew lounge, etc). The activation points must not be capable of deactivating the alarm once it has been initiated and it must be protected against inadvertent operation. Seals, lids or covers that must be broken, or buttons that remain depressed upon activation of the alarm, may not be used since a broken seal or depressed button would indicate that the alarm has been tripped. Spring loaded buttons, covers, or similar devices that provide no indication of the status of the alarm are acceptable. Activation of the SSAS should not cause any alarm or indication to be raised on the ship or near the activation point.
  - B. If the SSAS uses the ship's main source of electrical power, a suitable backup service should be provided to sufficiently and properly power the SSAS for at least 24 hours. This backup service may be an existing alternate source or dedicated battery backup. For these systems, an Uninterruptible Power Supply (UPS) or similar device powered from the ship's main power may be used for an alternate source of power.
  - C. The SSAS may be a component of existing radio installations but it may not interfere with the normal function of that equipment. If the SSAS uses any new radio transmission equipment or modifies existing radio transmission equipment (except for software modifications that do not affect transmission characteristics), then the Federal Communications Commission (FCC) must certify the equipment. Any new electronic

equipment must be certified by the manufacturer to comply with the relevant sections of IEC 60945<sup>1</sup> that are identified as being required for all equipment categories.

- D. The relevant CSP should certify specific SSAS equipment as acceptable if the alerts are processed via a maritime mobile satellite system.
- E. SSASs should generally meet the requirements and standards applicable to other distress alerting equipment as follows:
  - 1. SSASs that operate through the Cospas-Sarsat system should generally meet the relevant requirements for Electronic Position Indicating Radio Beacons (EPIRBs) contained in 47 CFR 80.1061, 1101, and 1103, and should be registered and labeled similar to the requirements for EPIRBs contained in 47 CFR 80.1061. These regulations establish requirements for radio emissions, test facility certification, submission of information to the Coast Guard and FCC, coding, labeling, and registration.
  - 2. SSASs that operate through the Inmarsat system should generally meet the relevant requirements for Inmarsat ship earth stations contained in 47 CFR 80.1101 and 1103. These regulations establish requirements for radio emissions, type approval by Inmarsat, and submission of information to the FCC for certification. Inmarsat SSASs should be registered with Inmarsat in accordance with IMO Assembly Resolution A.887 (21).
  - 3. SSASs that rely on encrypted terrestrial radio transmissions should be closely evaluated, and may be acceptable depending on the route of the vessel; however, if this approach were employed, encryption provisions satisfactory to the Coast Guard would have to be used with arrangements for maintenance of the encryption key.
  - 4. Other equipment proposed for use as SSASs on U.S.-flag vessels should also be certificated by the FCC and accepted by the Coast Guard for its intended use. How the equipment complies with the recognized national or international standards should be noted in the manufacturer's documentation provided with the equipment. Generally, such equipment should meet performance and registration requirements comparable to those cited for equipment operating through Cospas-Sarsat and Inmarsat as discussed above if maritime mobile satellite systems are used, or comparable to the relevant provisions of 47 CFR Part 80 for terrestrial systems. For vessels away from coastal areas, cellular phones and electronic mail are not generally considered suitable means of delivering ship security alerts to competent authorities due to typical limits on reliability and automatic processing.

---

<sup>1</sup> International Electrotechnical Commission (IEC) Publication IEC 60945 (2002) "Maritime navigation and radiocommunication equipment and systems – General requirements – Methods of testing and required test results"

5. Radio equipment used for SSASs may operate on appropriate emergency frequencies designated for distress communications.
9. Equipment Registration: Equipment should be appropriately registered to ensure that 24/7 arrangements are in place for retrieval of SSAS information by competent authorities. The registration data may be maintained by the CSP or other suitable entity and ideally should be retrieved automatically and forwarded with a ship security alert. The ship owners or operators are responsible for ensuring that this data is up-to-date.
10. Ship Security Alert Messages:
  - A. Alert messages should be generated automatically with no input from the operator other than the activation of the system, and must be capable of reaching the competent authority from any point along the vessel's intended route. This alert should not be transmitted as a general distress alert. Once activated, the SSAS should continue to transmit the security alert until the equipment is reset or deactivated. The interval between transmissions of the alerts should ideally be between 15 minutes and one hour. Ship security alert messages should only be sent to the shore stations that are outlined in the vessel security plan's SSAS annex. Ship security alert messages should not be sent to ship stations.
  - B. The format of ship security alerts should be compatible with the communication system used to transmit it and, as a minimum, contain the following:
    1. Ship's identity (e.g., IMO number, Inmarsat IDs (including ocean regions code), Maritime Mobile Service Identity (MMSI) number, or call sign);
    2. Ship's position (latitude and longitude associated with a date and time); and
    3. Ship's security alert activation indication.
  - C. Messages should be transmitted at distress priority (or priority 3 if the system transmits via Inmarsat).
  - D. Alert messages are difficult to validate because international regulations prevent direct contact with the vessel in question. However, investigation into the alert using sources on board the vessel is feasible if conducted properly. The IMO Maritime Safety Circular 1072, of 26 June 2003, allows a system that utilizes the exchange of messages containing key words between a ship and the ship's company via speech or data communications. In no instance will the U.S. Coast Guard directly contact the vessel during the initial investigation of an alert. Other actions that might help to validate an alert are:
    1. When predetermined check-in times are established, and a vessel misses a check-in which is immediately followed by an alert;

2. If a security alert is received in conjunction with a distress alert;
  3. If a partial, obscure, or incomplete transmission precedes a security alert; or
  4. If a predetermined "codeword" is received (keywords and/or phrases that under normal circumstances would be standard but may have alternate answers that would indicate a problem).
- E. Whatever mechanism is employed, its existence and format should be available only to a select number of persons on board the vessel and the entity (e.g. Ship's Company, TSP, or CSP) responsible for forwarding the alert to RCC Alameda. Additionally, these validation methods should not be used if they could endanger the crew or ship, or raise suspicion. The mechanism should be changed frequently, especially the use of a "codeword," and proper training should be conducted on a regular basis. Whatever mechanism is used to validate an alert, the details should be described in the SSAS Annex to the VSP. RCC Alameda should also be advised of the validation mechanism upon the initial investigation of a ship security alert.

11. Termination and Post Incident Reports:

- A. RCC Alameda is to be notified by the appropriate entity, such as the Company Security Officer (CSO), the vessel owner or owner's agent, or the competent authority (for foreign vessels) when an alerted security threat has ended. Additionally, it is important to report all threats to vessel security in which the ship's SSAS has been activated, whether successful or unsuccessful, to RCC Alameda. This information is used to reduce the risks of future incidents, improve preparedness to respond to such incidents, and enable the U.S. Government to comply with mandatory reporting requirements to the IMO.
- B. This post-incident report should be submitted in the following format:
1. Ship's name and call sign, IMO number, Inmarsat ID, or MMSI number;
  2. Reference initial ship security alert;
  3. Name of the area  
Position of incident (Latitude and longitude)  
Time of incident;
  4. Details of incident, e.g.,
    - While sailing, at anchor or at berth?
    - Method of attack
    - Description/number of suspect craft
    - Number and brief description of attackers/perpetrators
    - What kind of weapons did the attackers carry?

- Any other information (e.g., language spoken)
  - Injuries to crew and passengers
  - Damage to ship (Which part of the ship was attacked?)
  - Brief details of stolen property/cargo
  - Actions taken by the master and crew
  - Was incident reported to the coastal authority and to whom?
  - Action taken by the coastal state;
5. Last observed movements of pirate/suspect craft (e.g. Date/time/course/position/speed);
6. Assistance required;
7. Preferred communications with reporting ship, e.g.,  
Appropriate Coast Radio Station  
HF/MF/VHF  
INMARSAT IDs (including ocean region code)  
MMSI; and
8. Date/time of report (UTC).

12. Inadvertent or False Ship Security Alerts:

- A. The ship should report an inadvertent alert to RCC Alameda immediately to protect system integrity and to prevent a costly response that may divert response resources from a bona fide emergency.
- B. False alerts are extremely costly, occupying time and resources that become unavailable to respond to valid events. The Coast Guard intends to prosecute vessels or people making false alerts if it is determined that the false alerts are intentional. The nature of an alert and the response multiplies the effect of a false alert.

13. Communications Service Providers:

- A. A CSP receives radio security alerts from ships and relays them to either competent authorities, TSPs, or Flag Administrations using capabilities such as satellite systems, terrestrial radio systems, and ground communications links.
- B. Global Maritime Distress and Safety System (GMDSS)-based CSPs already operating as an IMO-recognized part of GMDSS need not undergo further approval to process ship security alerts as long as these alerts are handled in a manner equivalent to GMDSS distress alerts, and are routed to U.S. designated competent authorities.
- C. Non-GMDSS-based CSPs using mobile satellite systems not yet or not intending to be recognized by IMO as part of GMDSS will need to be reviewed by the U. S. Coast Guard

Enclosure (5) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 04-03

Office of Systems Engineering (CG-3PSE-3) for suitability with the applicable provisions of IMO Assembly Resolution A.888 (21). Non GMDSS-based CSPs will also need to be reviewed by the Federal Communications Commission (FCC). Non-GMDSS CSPs are to be capable of doing the following:

1. Provide continuous coverage in areas where ships using the system will sail with at least 99.9% network availability;
  2. Be able to handle the anticipated distress priority traffic by vessels using the system;
  3. Automatically route ship security alerts to the appropriate designated competent authorities or TSPs;
  4. If practicable, advise vessels, competent authorities, and TSPs of any outages or scheduled downtime before or when they occur; and
  5. Continuously monitor and record network availability and provide a report on the recorded availability to the Commandant (CG-3PSE-3) at least once every year.
- D. Store and forward systems should have arrangements in place to ensure that ship security alerts are promptly delivered.
- E. CSPs should make every effort to be able to provide current vessel critical data to RCC Alameda. The data should be maintained by the CSP or another suitable entity and, ideally, should be retrieved automatically and forwarded with a ship security alert. The data should include vessel information/identification and 24 hour contact information for a responsible person that may assist RCC Alameda in validating a ship security alert. If the data is maintained on a password protected website, arrangements will need to be made to provide RCC Alameda a login name and password to facilitate response efforts to an alert.
- F. A CSP should be able to demonstrate that they can reliably perform these functions without actually processing an alert through to the competent authority, i.e., it should be able to show upon request from a U.S. Coast Guard authority that it can automatically relay a message at the appropriate distress priority through its system up to the point where it is handed off to the next CSP or TSP in the system to the competent authority.
- G. Once a CSP is supporting the transmission and relay of ship security alerts for vessels, a two year written notice should be given to the U.S. Coast Guard and relevant vessel owners for the withdrawal of such services, unless vessels are no longer using the service or unless otherwise approved by the U.S. Coast Guard.

13. Tracking Service Providers (TSP's):

- A. A TSP monitors the transmission reports and receives the radio security alerts via the



CSP and informs competent authorities and the CSO when the transmission format changes.

- B. In such cases where the SSAS alert is sent only to the TSP and is not automatically routed to the competent authority, the TSP must show that it is in accordance with the applicable provisions of IMO Assembly Resolution A.888(21) and their ability to meet the guidelines in this section. The TSP's compliance statement must be submitted with the vessel's security SAS annex.
- C. In lieu of submitting all of the documentation to demonstrate compliance with the entire section 13A(1), TSPs already accepted/approved to receive GMDSS alerts are only required to submit documentation showing their GMDSS acceptance/approval. (TSPs accepted/approved to receive GMDSS alerts are already verified by the International Mobile Satellite Organization (IMSO)).
- D. TSPs should:
  - 1. Operate a dedicated watch in continuous operation 24 hours a day, seven days a week for 365 days a year;
  - 2. Be able to connect to RCC Alameda;
  - 3. Keep continuous watch on appropriate satellite communication channels; and
  - 4. Be capable of processing the information received with the highest priority.
- E. Priority:
  - 1. The TSP should be capable of automatically recognizing the priority of ship-to-shore communications and should preserve the priority and process maritime mobile communications for the following four levels of priority:
    - a. Distress;
    - b. Urgency;
    - c. Safety; and
    - d. Other communications.
  - 2. Priority access should be given for distress alerts and calls in real time.
  - 3. The TSP must have reliable communication links to RCC Alameda.
  - 4. The communication links for mobile-satellite voice communication systems, or data communications systems, should be connectable to the public switched network in accordance with relevant International Telecommunication Union (ITU) recommendations.

- F. U.S. Flagged vessels may be required during inspection and testing of their SSAS to provide adequate documentation proving that the CSP/TSP with which they have contracted, meets the requirements as above. The documentation will be kept by the vessel as part of its VSP with the details of system operation.
- G. Should a TSP that is supporting the transmission and relay of ship security alerts for vessels have to withdraw its services, the TSP must notify the U.S. Coast Guard and relevant owners of the withdrawal and allow sufficient time for the affected vessel(s) to obtain services from another CSP or TSP.

14. SSAS Inspection and Testing:

- A. The SSAS should be capable of being tested, upon request by a marine inspector, without inadvertently sending a live transmission. Procedures for testing should be outlined in the vessel's security plan. SSAS testing shall be logged in accordance with 33 CFR 104.235. Marine inspectors are not to send a live transmission to RCC Alameda when inspecting SSAS units aboard vessels.
- B. Testing procedures for SSAS systems are indicated by the type of SSAS system employed aboard the vessel. Coast Guard Inspectors or other approving officials must consult system documentation to determine if the unit is installed and functioning properly. The results of a successful test may be a message received at the vessel's CSP/TSP, an indicator light upon the unit itself, or the reception of routine fleet management data from the unit. In general, the testing procedures should be carried out according to the following (or equivalent) procedures, as appropriate for the particular SSAS:
  - 1. Carry out a self-test routine for internal circuitry and emissions, in accordance with the SSAS manufacturer's instructions or handbook;
  - 2. Confirm that the system is properly registered; and
  - 3. Check the battery expiration date, if applicable.

**ENCLOSURE 6**

**GUIDANCE FOR SUBMISSION OF  
ALTERNATIVE SECURITY PROGRAM (ASP),  
WAIVERS, AND EQUIVALENCIES**

1. **Alternative Security Program (ASP), Waiver, and Equivalency Submissions**

- A. The Final Rules published October 22, 2003 addressing the implementation of the Maritime Transportation Security Act of 2002 (MTSA) and the International Ship and Port Facility Security (ISPS) Code permits trade organizations or industry groups representing owners or operators to request approval for the use of an Alternative Security Program (ASP). The approved ASP must address all requirements in 33 CFR Part 104 as applicable. ASPs that will be used throughout a sector of the industry must be submitted and approved within a timeframe that allows owners or operators to choose between implementing the applicable ASP and implementing an individual security plan. An ASP may also be used when an owner or operator intends to use a single plan to cover multiple terminals and vessels where exclusive docking arrangements exist. When an ASP is used for this purpose, a covered vessel would not be able to use an "outside" facility and a covered facility would not be allowed to receive an "outside" vessel.
- B. Owners or operators may request approval for a waiver of security requirements in accordance with 33 CFR 104.130. A waiver may be requested for any requirement that the owner or operator feels is unnecessary in light of the operating conditions of the vessel. The request should articulate the reason why a specific requirement is unnecessary (i.e., it should explain the circumstances that exist, which cause the requirement to be unnecessary). If approved the waiver should be incorporated into the Vessel Security Plan submitted to the MSC. Owners and operators that participate in an approved ASP, will not be granted a waiver because the ASP must be implemented in its entirety.
- C. Owners or operators may also request approval for equivalent security measures in accordance with 33 CFR 104.135. A request should include information to assist Commandant (G-MPS-1) in assessing the effectiveness of the proposed equivalent security measure. Equivalent measures that are approved should be incorporated into the Vessel Security Plan submitted to the MSC. Owners and operators that participate in an approved ASP, will not be granted a waiver because the ASP must be implemented in its entirety.

2. **General Guidance**

- A. ASPs, waivers, or equivalencies and any accompanying documents must be submitted via hard copy paper document, floppy disc, or compact disc (CD). Vessel security plans (VSP), facility security plans (FSP), and ASPs are deemed to contain Sensitive Security Information (SSI) and shall not be submitted to the Coast Guard via E-mail. They must be mailed to:

Commandant, U. S. Coast Guard (G-MPS)  
2100 Second Street S.W.  
Washington, DC 20593-0001

- B. Each package must contain:
- Point of contact,
  - Mailing address, and
  - Telephone number.
- C. Operational Security. Security plans, including Vessel Security Plans, Facility Security Plans, and ASPs, are considered to be Sensitive Security Information (SSI), and therefore, they are exempt from the Freedom of Information Act (FOIA), meaning that FOIA requests for ASPs will likely be denied. Any requests for such documents, however, should be forwarded to the applicable FOIA Officer and the G-MP legal advisor for decision and action.
- D. Telephonic, E-Mail, And Face-To-Face Inquiries. The regulations addressing security requirements are lengthy, complex, and vary in application from vessel to vessel, facility to facility, and port to port. Therefore, it is preferable that exchanges regarding regulation application take place in writing. Members of the public with specific applicability questions should submit their inquiries via letter or E-mail. Once the issue is properly researched, a written response will be provided. A list of Frequently Asked Questions (FAQs) and their answers, will be posted on the USCG Port Security Directorate website <http://www.uscg.mil/hq/g-m/mp/index.htm>, to assist the public. A Help Desk has been established to assist the public with inquiries. The phone number for the Help Desk is 202-366-9991 and will be manned Monday through Friday from 0800 to 2000 hours Eastern Standard Time.

### **3. ASP Application Requirements**

- A. ASPs that apply to an individual owner or operator must be submitted no later than December 31, 2003. Each ASP must contain:
1. A list of the vessel and/or facility types to which the ASP will apply.
  2. A security assessment for the vessel and/or facility types.
  3. An explanation of how the ASP addresses the requirements contained in 33 CFR Parts 104, 105, and/or 106, as applicable.
  4. A specific explanation of how the owner and/or operator will implement each portion of the ASP. The ASP must explain which parts of the plan are applicable to various facilities, and require facility owners to activate/implement each part of the plan that applies to that type of facility.
  5. We recommend including an index cross-referencing applicable sections of the regulations with the specific paragraphs or sections of the ASP.
- B. An ASP that only addresses intended alternatives is not sufficient.

### **4. Action Upon Receipt of an ASP Submission**

- A. Applications will be reviewed on a first-come, first-served basis. The submission process is outlined in figure (1) below.

- B. Each application will undergo an initial review to ensure each required subject area is addressed. To pass initial review an ASP must meet qualifications requirements in 33 CFR 101.120, and must address all items of either 33 CFR 104.405 or 33 CFR 105.405 as appropriate. If the application is lacking critical information, it will be disapproved and the Coast Guard will send the submitter a letter containing a brief explanation of the reasons for disapproval. Coast Guard Headquarters (G-MPS) will retain the application and related material for future reference.

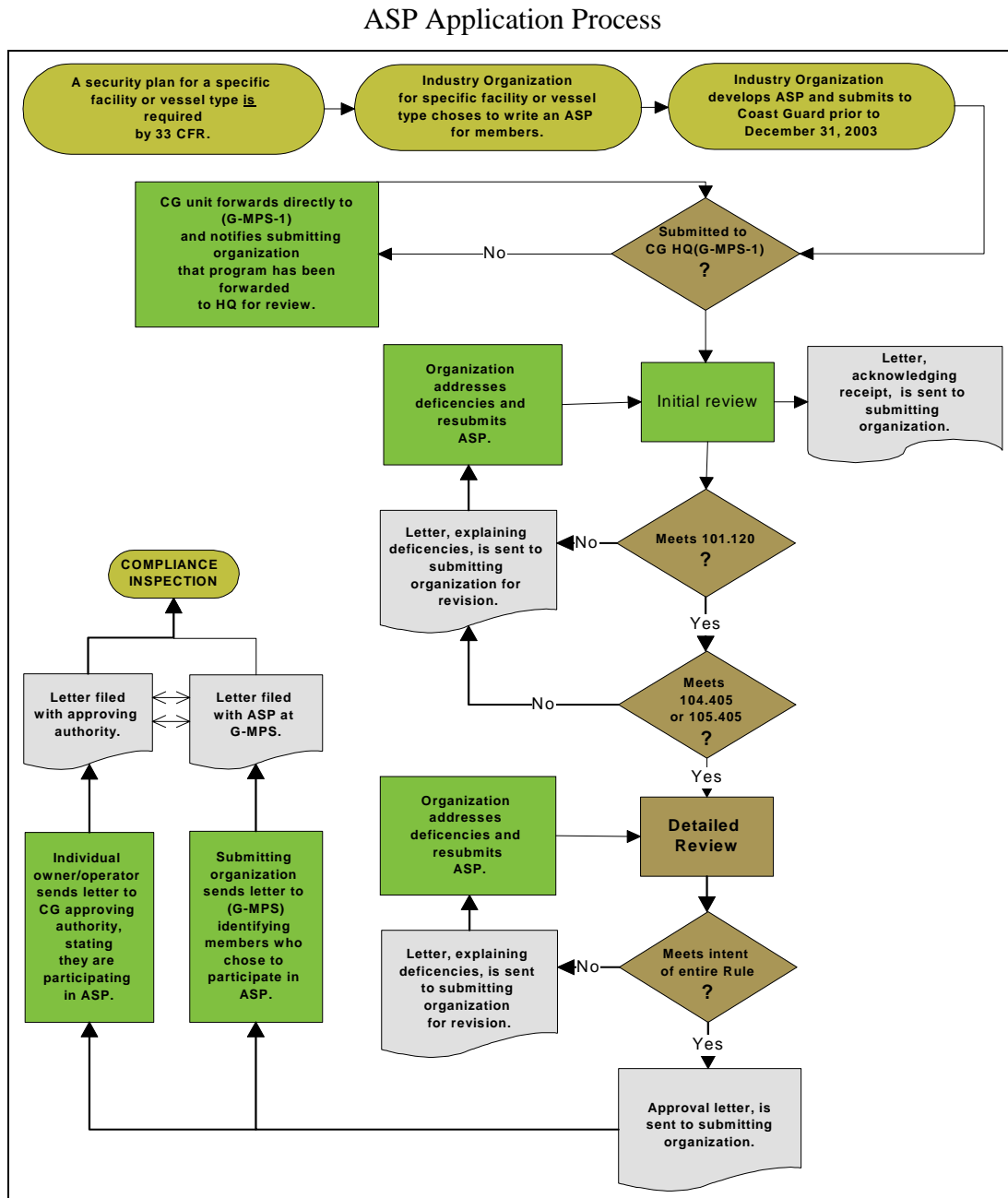


Figure 1

- C. Applications that pass the initial review will then undergo a detailed review. During this phase the ASP is reviewed to determine if it meets the intent of the entire rule for its specific industry type. The ASP content will be examined to determine compliance with all performance standards and at all MARSEC levels.
- D. If the application is approved after the detailed review, a letter will be mailed to the submitter stating its acceptance and any conditions that may apply. Coast Guard Headquarters (G-MPS) will retain and file the application.

If the application is not approved, a copy of the application will be returned to the submitter with a brief statement why it cannot be approved. The original application will be kept on file at Coast Guard Headquarters (G-MPS) for future reference. The organization may make corrections and resubmit the program.

## **5. ASP Compliance**

- A. On or before December 31, 2003, a vessel owner or operator using an ASP must send in a letter to Marine Safety Center stating which approved ASP they are intending use to:

Commanding Officer  
Marine Safety Center  
Room 6302  
400 Seventh Street S.W.  
Washington, D.C. 20590

- B. On or before July 1, 2004, a vessel owner or operator must have a copy of the ASP the vessel is using, including a vessel security assessment report and a letter signed by the vessel owner or operator stating which ASP the vessel is using and certifying that it is in full compliance with the program.
- C. An ASP on an individual vessel is an element of a larger security program. Owners or Operators that are using an ASP must remain members of the organization that sponsored the ASP in order to receive updates and amendments. Inspectors may verify that a vessel has maintained its membership checking for membership certificates, letters, or online databases if available. If no evidence exists that the vessel is a current member, the burden of proof rests on the owner or operator.

## **6. Equivalency and Waiver Application Requirements**

- A. Equivalency Requests. For any security measure required by 33 CFR 104, the owner or operator may apply for approval to substitute an equivalent security measure that meets or exceeds the effectiveness of the required measure. G-MPS personnel will assess the adequacy of each equivalency request. Each application must contain:

- 1. The request to use an equivalent security measure.

2. The documentation supporting justification for the request.
- B. Waiver Requests. Owners or operators are permitted to apply for a waiver of any requirement in 33 CFR 104, 105, or 106, that the owner or operator considers unnecessary in light of the nature or operating conditions of the vessel or facility. G-MPS personnel will assess the adequacy of each waiver request. Each application must contain:
1. The request for the waiver to a requirement.
  2. The documentation supporting justification for the request, e.g., vulnerability assessment information, if available; a description of the vessel type, certification status and operation; information on the extent of physical transfer of fuels, supplies or cargoes; information on facilities called by the vessel; any applicability issues; any information on security measures already in place.
- C. Documentation. Requests for equivalencies and/or waivers should include, as applicable, the following: vulnerability assessments, if available; a description of the vessel type, certification status and operation; cargoes carried; details regarding physical transfer of fuels and supplies; crew size, if manned; details regarding waterways used and facilities used by the vessel; applicability issues, if any; and details of security measures already in place.

**7. Action Upon Receipt of a Waiver or Equivalency Request**

- A. Upon receipt a letter will be sent to the owner or operator from G-MPS acknowledging receipt of the equivalency or waiver request. In the letter the owner or operator will be directed to continue working on the facility or vessel security plan. The submission process is outlined in figure (2) below.
- B. Applications will be reviewed on a first-come, first-served basis.
- C. Each application will undergo an initial review to ensure each required subject area is addressed. If the application is lacking critical information, it will be disapproved and the Coast Guard will send the submitter a letter containing a brief explanation of the reasons for disapproval. Coast Guard Headquarters (G-MPS) will retain the application and related material for future reference.
- D. Applications that pass the initial review will then undergo a detailed review. Coast Guard Headquarters (G-MPS) will normally request further review and input from the appropriate Area Commander. The Area Commander may disseminate for review as appropriate. All comments will be returned to G-MPS. During the detailed review, the content of the request will be examined to determine compliance with the performance standards at all MARSEC levels.



- E. If the application is approved after the detailed review, a letter will be mailed to the submitter stating its acceptance and any conditions that may apply. Coast Guard Headquarters (G-MPS) will retain and file the application.
- F. If the application is disapproved after the detailed review, a copy of the application will be returned to the submitter with a brief statement of the reasons for disapproval. The original application will be kept on file at Coast Guard Headquarters (G-MPS) for future reference.

Waivers and Equivalencies Approval Process

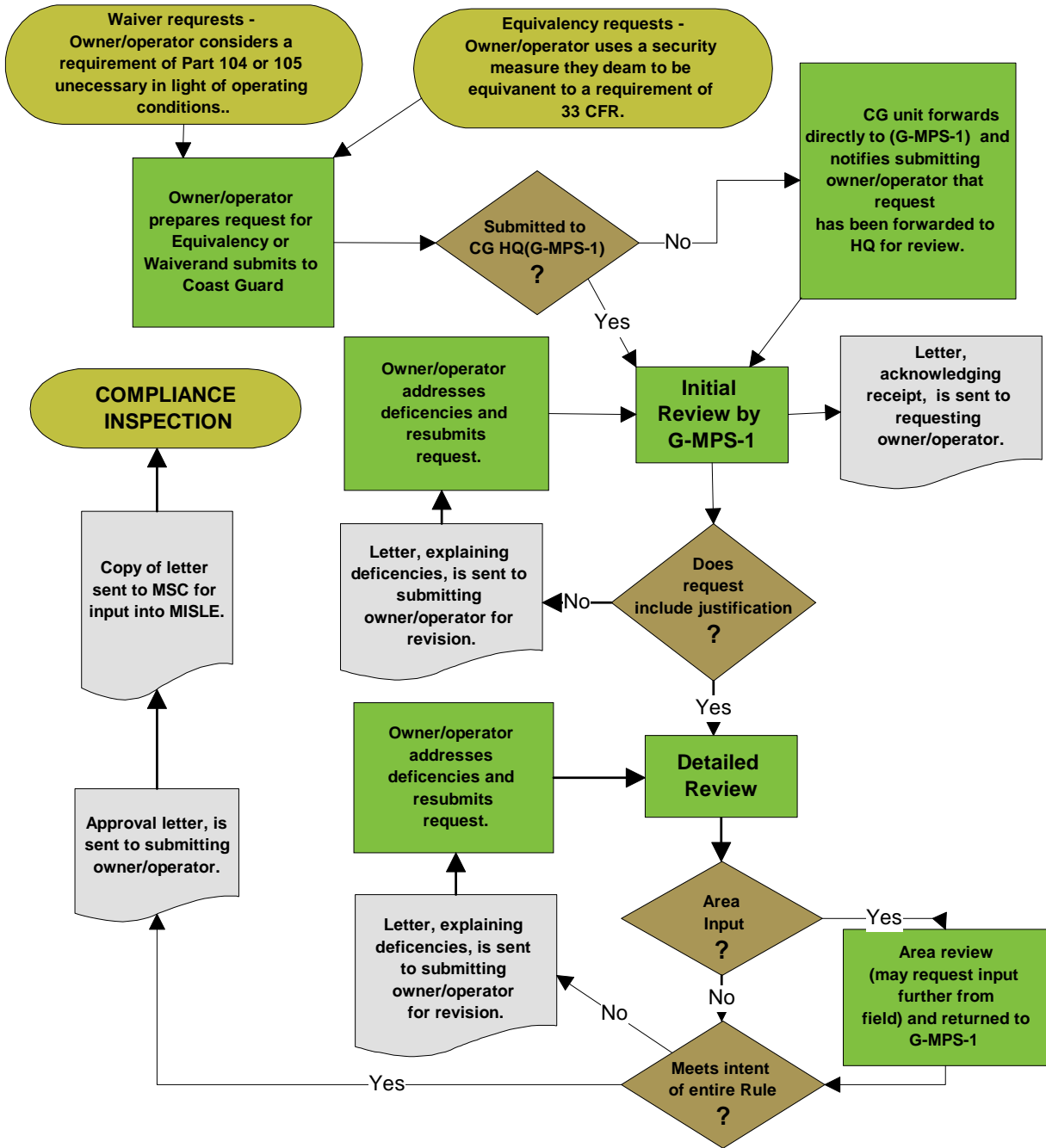


Figure 2

**ENCLOSURE (7)**

**DOMESTIC VESSEL SECURITY PLAN  
VERIFICATION GUIDE FOR MTSA/ISPS CODE**

A bi-fold version of this checklist is available on the intranet at <http://cgweb.comdt.uscg.mil/G-Mp/pdf/840%20Style.pdf>

*United States Coast Guard*



**DOMESTIC VESSEL SECURITY PLAN  
VERIFICATION GUIDE FOR MTSA/ISPS CODE**

<b>Name of Vessel</b>	<b>Vessel Type</b>								
<b>Documentation Number</b>	<b>Case Number</b>								
<b>Date Completed</b>									
<b>Location</b>									
<p><b>Senior Marine Inspectors / Boarding Officers</b></p> <table style="width: 100%; border: none;"> <tr> <td style="width: 50%; border: none;">1. _____</td> <td style="width: 50%; border: none;">5. _____</td> </tr> <tr> <td style="border: none;">2. _____</td> <td style="border: none;">6. _____</td> </tr> <tr> <td style="border: none;">3. _____</td> <td style="border: none;">7. _____</td> </tr> <tr> <td style="border: none;">4. _____</td> <td style="border: none;">8. _____</td> </tr> </table>		1. _____	5. _____	2. _____	6. _____	3. _____	7. _____	4. _____	8. _____
1. _____	5. _____								
2. _____	6. _____								
3. _____	7. _____								
4. _____	8. _____								

### **Use of Domestic Vessel Security Plan Verification Guide for MTSA/ISPS Code.**

This guide is designed to assist the Coast Guard Inspector in conducting a field verification of the vessel security plan of a U.S. Flagged vessel<sup>1</sup>. This booklet is divided into three sections. Section (A) contains spaces for the vessel particulars that are needed to complete an activity in MISLE for vessels on an international voyage. Section (B) is a guide to the parts of the regulations or Code and is designed to be used as a checklist when verifying the VSP. The inspector should complete the checklist by consulting the VSP for specific security measures. Section (C) is designed to provide additional information to the inspector. This section may be discarded as the inspector gains experience conducting verification exams. A bi-fold booklet is also provided on the G-MP MTSA/ISPS information website at <http://cgweb.comdt.uscg.mil/G-Mp/index.html>.

There are three key steps that the Coast Guard inspector must follow in conducting a verification:

- Ensure the vessel complies with the Vessel Security Plan (VSP).
- Ensure the adequacy of the vessel security assessment (VSA).
- Ensure that the measures in place adequately address the vulnerabilities.

MTSA regulations do not mandate specific equipment or procedures, but call for performance based criteria to ensure the security of the vessel. While this guide is designed to assist the Coast Guard inspector, this guide cannot be used alone to verify the vessel has adequate security measures. The review of the VSP and the VSA require interaction with company and/or vessel when conducting a verification aboard the vessel.

Some domestic vessels that sail on international routes will also be required to meet the International Ship & Port Facility Security (ISPS) Code. The Coast Guard as the representative of the Contracting Government<sup>2</sup> must verify that the vessel fully complies with the ISPS Code prior to issuing the International Ship Security Certificate (ISSC). The Maritime Transportation Security Act (MTSA) and the corresponding regulations also require compliance for a vessel to operate, but do not require a certificate to be issued. However, MTSA<sup>3</sup> like ISPS requires the Coast Guard to verify that that vessel is in compliance with an approved security plan. Because MTSA encompasses the requirements of ISPS, compliance with MTSA satisfies ISPS requirements except as noted for U.S. flag vessels on an international route

MTSA and ISPS place the responsibility to complete an accurate security assessment, and to address the vulnerabilities in the Vessel Security Plan (VSP), or Ship Security Plan (SSP)<sup>4</sup> on the owner or operator of a vessel. The Coast Guard has the responsibility to verify that the vessel is complying with its approved plan.

#### **Pre-inspection Items**

- Review MISLE records
- Deficiency History
- Critical Profile
- CG Activity History

#### **Inspection Items**

- Review VSP
- Review VSA Report
- Conducted verification with exam booklet and VSP

#### **Post-inspection Items**

- Issue/endorse certificates to vessel
- MISLE activity case

<sup>1</sup> This guide may also be used for the small number of foreign flagged vessels, such as non-SOLAS foreign vessels subject to MTSA.

<sup>2</sup> The term "Contracting Government" used in the ISPS Code means the Flag State, and for the purposes of this circular means the Coast Guard on behalf of the United States..

<sup>3</sup> For the purposes of this circular, the term MTSA means the MTSA regulations and the term ISPS means the ISPS Code unless otherwise noted.

<sup>4</sup> For the purposes of this circular, unless otherwise noted when the requirements for the Vessel Security Plan (VSP) or Vessel Security Assessment (VSA) are discussed, it includes the similar requirements for the Ship Security Plan (SSP) or Ship Security Assessment (SSA), respectively, which are required by the ISPS Code.

This section is only required for U.S. Flag vessels on an international voyage.

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)							

### Equipment Data

Equipment Type	Description	Approval Information	Authority/Agency
AIS Communications			
Ship Security Alert System			

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

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

(1) as defined in SOLAS Chapter IX

Security Personnel (Compare to Current MISLE Data)

CSO Name:	VSO Name:
CSO Contact Number:	VSO Contact Number:
CSO Address:	VSO Address:

Section A  
Certificates/Equipment  
Data/Records Information

Section B  
U.S. Flag Vessel MTSA/ISPS Code Exam Booklet  
Security Practices and Crew Competencies

Examinations shall address all areas of the MTSA regulations and certain ISPS requirements as appropriate, and shall be done through: observation that security procedures are in place; questioning crewmembers regarding security duties and security procedures; verifying on board presence and validity of required security documents and certificates; and proper operation of security equipment. This booklet includes several job aids to assist with these processes. This booklet is intended to be used as a guide to general MTSA requirements, and specific requirements will be contained in the VSP.

- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Compliance documentation</li> <li>• Approved Vessel Security Plan               <ul style="list-style-type: none"> <li>○ Review the VSP</li> <li>○ Review the Vessel Security Assessment</li> </ul> </li> <li>• Letter from MSC stating under review</li> <li>• Alternative Security Plan, with letter signed by vessel owner/operator.               <ul style="list-style-type: none"> <li>○ Review ASP and vessel assessment - ASP used:<br/>                 _____</li> </ul> </li> </ul>   | <p>33 CFR 104.120<br/>ISPS, Part A, 9.1</p>   |
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Noncompliance</li> <li>• Conditions in place (if any)</li> <li>• Conditions met</li> <li><input type="checkbox"/> Waivers.</li> <li>• Waiver approval letter from G-MP</li> <li><input type="checkbox"/> Equivalents</li> <li>• Approved by G-MP</li> <li><input type="checkbox"/> Alternative Security Programs.</li> <li>• Updated</li> <li>• Plan on board manned vessels?</li> <li><input type="checkbox"/> Maritime Security (MARSEC) Directive.</li> <li>• Proper safeguards</li> <li>• Incorporated in to security plan</li> <li><input type="checkbox"/> Master.</li> <li>• Aware of responsibility and authority with regards to MTSA</li> <li><input type="checkbox"/> Company Security Officer (CSO)</li> <li>• Training /Experience</li> <li>• See list of sample questions</li> <li><input type="checkbox"/> Vessel Security Officer (VSO)</li> <li>• See list of sample questions</li> <li>• Training and experience</li> </ul> | <p>33 CFR 104.125</p> <p>33 CFR 104.130</p> <p>33 CFR 104.135</p> <p>33 CFR 104.140</p> <p>33 CFR 104.145</p> <p>33 CFR 104.205</p> <p>33 CFR 104.210<br/>ISPS, Part A, 11.1</p> <p>33 CFR 104.215<br/>ISPS, Part A, 12.1</p> |



- |   |   |
|---|---|
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Company or vessel personnel with security duties</li> <li>• See list of sample questions</li> <li>• Training and experience</li> </ul>  | <p>33 CFR 104.220<br/>ISPS Part A, 13.1</p>   |
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Security training for all other vessel personnel</li> </ul>   | <p>33 CFR 104.225<br/>ISPS Part A, 13.1</p>   |
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Drill and exercise requirements</li> <li>• Conducted drill to test individual elements of the security plan</li> <li>• Security incident procedures</li> <li>• Tests response to security incident in accordance with plan</li> <li>• Critique drill with VSO</li> <li>• Identify any deficiencies with the VSP determined by drill.</li> <li>• Frequency</li> </ul>  | <p>33 CFR 104.230<br/>ISPS Part A, 13.5</p>   |
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Vessel record keeping requirements</li> <li>• Training</li> <li>• Drills and exercises</li> <li>• Transportation Security Incidents</li> <li>• Breaches of security</li> <li>• Changes in Maritime Security (MARSEC) Levels</li> <li>• Maintenance, calibration, and testing of security equipment</li> <li>• Security threats</li> <li>• Annual audit of the VSP</li> <li>• Declaration of Security (DoS)</li> <li>• Retained for two years</li> </ul> | <p>33 CFR 104.235<br/>ISPS, Part A, 10.1</p>  |
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Maritime Security (MARSEC) Level coordination &amp; implementation</li> <li>• Proper MARSEC Level</li> <li>• MARSEC level at least at current port level</li> </ul>   | <p>33 CFR 104.240</p>                         |
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Communications</li> <li>• Vessel security personnel</li> <li>• Facility</li> <li>• National and local authorities</li> <li>• Demonstrate communications operations consistent with VSP</li> </ul>   | <p>33 CFR 104.245<br/>ISPS, Part A, 7.2.7</p> |
| <ul style="list-style-type: none"> <li><input type="checkbox"/> Declaration of Security (DoS)</li> <li>• Required for cruise ships or manned CDC bulk vessels and any vessel or facilities it interfaces with. Unmanned vessels do not require DOS.</li> <li>• Valid (for MARSEC level and effective time period)<br/>Must have last ten or Continuing DOS reviewed at interval consistent with MARSEC level</li> <li>• Signed</li> </ul>   | <p>33 CFR 104.255<br/>ISPS, Part A, 5.1</p>   |

- Security systems and equipment maintenance 33 CFR 104.260
  - Testing completed IAW manufacturer's recommendation
  - Working properly, effectively functions in accordance with the VSP
  - Ship Security Alert System (SSAS)
  
- Security measures for access control. 33 CFR 104.265  
ISPS, Part A, 7.2.2
  - Access points examined – signs posted in conspicuous locations
  - Control areas for authorized dangerous substances/devices
  - Means of identifying unauthorized personnel
  
- Security measures for restricted areas. 33 CFR 104.270  
ISPS, Part A, 7.2.4
  - Secure areas protected
  - Properly marked
  - Control measures adequate
  - Do not conflict with safety measures
  
- Security measures for handling cargo 33 CFR 104.275  
ISPS, Part A, 7.2.6
  - Identifying cargo tamper
  - Identifying approved cargo
  - Access point - inventory control
  - Checking cargo for dangerous substances
  
- Security measures for delivery of vessel stores and bunkers. 33 CFR 104.280  
ISPS, Part A, 7.2.6
  - Security procedures followed
  - Standing agreements valid
  
- Security measures for monitoring 33 CFR 104.285  
ISPS, Part A, 7.2.5
  - In accordance with VSP
    - Lighting
    - Test intrusion alarms
    - Emergency search procedures
  
- Security incident procedures 33 CFR 104.290
  - Witness during drill
  
- Additional requirements for passenger vessels and ferries 33 CFR 104.292
  
- Addition requirements for cruise ships 33 CFR 104.295
  
- Additional requirements--vessels on international voyages. 33 CFR 104.297  
ISPS, Part A, 19.1  
SOLAS XI-2, Regulation 5.4.1
  - ISSC issued
  - CSR updated

Note: The vessel may not have a CSR for the initial verification exam.

Vessel Security Assessment Report 33 CFR 104.300

- Reviewed and attached to VSP

Vessel Security Plan 33 CFR 104.400

- Reviewed
- Onboard manned vessels

Amendment and audit. 33 CFR 104.415

- CSO/VSO audit letter attached to VSP as required
- Audits conducted as required  
(Annually)  
(After vessel modifications)

Ship Security Alert System (vessels subject to SOLAS only) ISPS Part A, 9.4.18  
SOLAS XI-2, Regulation 6

- On the bridge and one other location
- Designed to prevent inadvertent activation
- Covert (unmarked, silent, and need to know)
- Tested IAW VSP

Comments:

- Security Drill
- Observe security drill exercising the activation of the provisions in the VSP related to a security threat, breach, security communications, change of security level, or other security related incident or action as described in the VSP
  - Drill selection and location shall be as directed by the Master and VSO. Describe:

---

---

---

---

---

---

---

---

---

---

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 the provisions of the Maritime Transportation Security Act, 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 to determine that personnel are properly trained and that meaningful security procedures are in place.

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? 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 VSP 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 Vessel Security Plan?

To Crew members having security responsibilities:

Who is the Vessel 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 Vessel Security Officer?  
What do you do if there is a security breach? Or security threat?

<p>Section C Additional Information</p>
---

Compliance documentation.

33 CFR 104.120  
ISPS, Part A, 9.1

*Inspectors may ensure the validity and accuracy of compliance documentation during the course of vessel inspections. When the VSP is not approved, the attending inspector may verify the existence of an acknowledgement letter from the MSC stating that the plan is currently under review. The vessel may continue to operate so long as it is in full compliance with the submitted plan. The inspector should issue a “no sail” requirement or COTP order after consulting the OCMI or COTP if the vessel does not have any of the required documentation*

*For vessel operating under an Alternative Security Program (ASP), the inspector should verify that a copy of the Coast Guard approved Alternative Security Program is available and that the ASP includes:*

- *a specific security assessment report.*
- *a letter from the owner or operator certifying which ASP is being used, and that the facility or vessel is in full compliance with that program.*
- *A COTP letter specifically authorizing the facility to operate.*

*Foreign Non-SOLAS Vessels:*

*For foreign vessels not subject to SOLAS Chapter XI, the inspector may verify:*

- *a valid letter from MSC attesting to the vessel’s compliance with 33 CFR 104 along with an approved VSP.*
- *An approved ASP along with a letter from the master that the vessel is in full compliance with the security plan may also be accepted.*
- *A valid ISSC certificate.*

*Unmanned Vessels:*

*Approval letters (for VSP or ASP) for unmanned vessels are required by regulation to be carried on board. However, as required by regulation, the VSP / ASP should not be maintained on board the vessels, but must be maintained in a secure location. During scheduled inspections, the plans must be made available to the Coast Guard upon request.*

*When scheduling inspections, the inspector should coordinate with owner/operators to ensure VSP/ASP availability at the time of inspection.*

*International Ship Security Certificate-ISSC (U.S. SOLAS Vessels only):*

*This document will be issued by the local OCMI following a satisfactory initial, or renewal verification of the VSP. The certificate carries a 5-year expiration date and has a minimum provision for one periodic verification.*

*Continuous Synopsis Records-CSR (U.S. SOLAS Vessels only):*

*The CSR should be accurate and reflect current vessel information. Updates to vessel files may be required. Discrepancies found in the CSR should be reported to the vessel master and/or owner so that corrective actions can be taken.*

Noncompliance.

33 CFR 104.125

*A noncompliance may be viewed similar to deviation from the 33 CFR 164 regulations. The COTP must decide if noncompliance represents a significant risk, and issue a COTP order to suspend operations or give COTP written authority to continue operations. If the condition is to persist while the vessel is transiting other COTP zones, each COTP or, in cases covered under 33 CFR 106.120, the cognizant District Commander, may agree to the measures imposed, consider additional measures, or prohibit entry until the deficiency is corrected.*

Waivers.

33 CFR 104.130

*The inspector will need to examine the waiver approval letter and verify that any conditions expressed are implemented. Since the condition placed on the waiver is meant to ensure the overall security of the vessel, the letter must be fully implemented. A vessel that is using an ASP is not eligible to request a waiver, since the regulations require an ASP plan to be implemented in its entirety.*

Equivalents.

33 CFR 104.135

*The inspector will need to examine the approval letter of any equivalencies that may exist. Equivalencies granted after the security plan has been approved should be noted in an amendment to the plan. Vessels that are using an ASP may not use an equivalency, since the regulations require the ASP plan to be implemented in its "entirety".*

Alternative Security Programs.

33 CFR 104.140

*An inspector of a vessel covered under an Alternative Security Program (ASP) approved by the Commandant (G-MP) should find that a copy of the ASP is on site. In addition, there should be a copy of the letter sent by the company to the appropriate plan approval authority identifying which ASP they have implemented, which vessels are covered and attesting that they are in full compliance with the ASP. It will be the responsibility of the individual performing the on-site inspection to confirm that the vessel, in compliance with the Alternative Security Program as it was approved, including any conditions of approval stipulated by the Commandant (G-MP), and in its entirety.*

*An area where an inspector would see an appropriate departure from a strict interpretation of the guidelines in 33 CFR parts 104 and 105 involves joint vessel/facility ASP's. In those cases where both the vessels and the facilities serving those vessels are owned and/or operated by the same entity, an alternative plan may recognize that the same party is responsible for security in both areas and approve an approach that addresses vulnerabilities and mitigation strategies for the vessels and the facility under the umbrella of one ASP. The practical result will be that the inspector will not be using separate plans for the vessels and the facility to determine compliance and, likewise, will not see some citations addressed in the plan if they are redundant between 104 and 105.*

Maritime Security (MARSEC) Directive.

33 CFR 104.145

*Inspectors must have a thorough knowledge of the MARSEC Directives that have been issued, and how they may affect the vessels in their respective COTP/OCMI zones. It will be incumbent upon the inspector to ensure that vessels that are affected have incorporated the MARSEC Directives into their security plans and measures.*

Company Security Officer (CSO).

33 CFR 104.210  
ISPS, Part A, 11.1  
ISPS, Part B, 8,9 & 13

*If the company has multiple CSO or if the CSO has delegated his/her duties in accordance with the regulations, the inspector may make inquiries of the designated crewmember to ensure that they understand that the ultimate responsibility rests with the CSO. In particular, an effective communication arrangement would be necessary to comply with the intent of the regulations. The CSO may demonstrate satisfactory knowledge of the VSP by asking questions such as:*

- *Describe the security organization of the company and its vessels*
- *How do you keep your company's vessels apprised of changing security levels?*
- *Have any problems or deficiencies been identified during annual audits?*

Vessel Security Officer (VSO).

33 CFR 104.215  
ISPS, Part A, 12.1  
ISPS, Part B, 8,9 & 13

*Inspectors may evaluate the ability of the VSO to perform the required duties and responsibilities in relation to: other assignments within the organization; multiple facility assignments; and retention of responsibility for delegated duties.*

*Inspectors may request confirmation that the qualifications of the VSO are substantially consistent with the requirements.*

*Inspectors may measure the performance of the responsibilities of the VSO required by the regulations by interviewing relevant personnel, reviewing records and documents required under this part, observation of drills, exercises, and actual incidents.*

*The inspector should issue a "no sail" requirement or COTP order after consulting the OCMI or COTP if the vessel does not have a designated VSO on board a manned vessel.*

Company and vessel personnel with security duties.

33 CFR 104.220  
ISPS Part A/B, 13.1

*The inspector may ask the crew to verify that they have knowledge of the required information through observation and conversation with the crewmembers regarding their security responsibilities. The questions may be kept informal, but should probe the depth of knowledge that an individual possesses concerning their assigned job. The questions may be directed at the security threats that the person may be expected to encounter, such as what type of behavior(s) would be considered "suspicious" when passengers are boarding the vessel. Although the average crewmember does not need to (nor should not) know the entire security plan, the ability to identify the CSO, or VSO and the aspects of the security plan that pertain to his/her station would demonstrate sufficient knowledge of the relevant sections.*

Security training for all other vessel personnel.

33 CFR 104.225  
ISPS Part A/B, 13.1

*The inspector may verify that others on a vessel are adequately trained by direct observation and questioning, but at a reduced level from the crew.*

*The inspector should also make use of personnel training records required under separate regulations.*

Drill and exercise requirements.

33 CFR 104.230  
ISPS Part A/B, 13.5

*The drill should demonstrate proper performance of the VSP. Each crew member may demonstrate their competency during the course of the drill. The inspector should critique the drill with the VSO, and discuss corrective action if necessary to address any deficiencies noted. Any deficiencies with the VSP detected during the drill may be corrected by directing the owner in writing to submit an amendment per the regulations. Such a requirement should be allowed at least 60 days. The inspector should issue a "no sail" requirement or COTP order after consulting the OCMI or COTP if in the opinion of the inspector, the measures contained in the VSP are not demonstrated by the crew due to their training, knowledge, or if an the number of crewmembers is insufficient to accomplish the security measure.*

*The inspector may accept proof of participation in an Area Maritime Security exercise to meet the requirement for an annual exercise if the owner furnishes proof of participation.*

Vessel record keeping requirements.

33 CFR 104.235  
ISPS, Part A/B, 10.1

*Inspectors should ensure that the VSO maintains the required records for security related evolutions such as training, drills and exercises, security threats, and maintenance of security equipment. These records may be kept in paper or electronic format and must be protected from unauthorized access or disclosure. The ISPS Code, part A requires that vessels subject to ISPS maintain records on board the vessel (Note: from Preamble). All other vessels record categories (except the Declaration of Security (DoS) on manned vessels) need not be stored onboard, but must be made available to the Coast Guard upon request.*

Maritime Security (MARSEC) Level coordination and implementation.

33 CFR 104.240

*Inspectors need to be aware of the prevailing MARSEC Level before they visit a vessel, as this will determine which security measures will be in place at the time of inspection. For example, if the port is at MARSEC Level 2 or 3 the vessel should have in place all the security measures required by their plan for at MARSEC Level 1, plus the measures required by the higher MARSEC Level. A vessel may not suspend operations to avoid enacting a measure described in the VSP unless this option is a specific provision of the VSP. Of course, an owner or operator may suspend operations at any time to protect the security of the vessel or operation.*

Communications.

33 CFR 104.245  
ISPS, Part A, 7.2.7

*Inspectors should examine the communication systems and procedures established under the VSP. Inspectors may question the VSO to ascertain the adequacy of provided communication equipment and procedures, and testing may be necessary. Communications will be considered effective if the VSO can demonstrate operation.*

Declaration of Security (DoS).

3

3 CFR 104.255  
ISPS, Part A/B, 5.1

*Inspectors should ensure adequacy of procedures for requesting and handling requests for DoS requests; review current and historical records for adequacy of DoS's, including signatures of VSO, FSO, their designated representatives and MARSEC level. Inspectors should also observe vessel and facility operations to ensure compliance with the DoS. The inspector should issue a "no sail" requirement or COTP order after consulting the OCMI or COTP if the required DoS are not on board. The vessels class society may be required to conduct an ISM audit to address this deficiency and prevent future Port State Control actions in foreign ports.*

*In addition, inspectors should verify that continuing DoS's have not exceeded the required time periods (90 days MARSEC 1, 30 days MARSEC 2 and no continuing DoS authorized for MARSEC level 3).*

Security systems and equipment maintenance.

33 CFR 104.260

*Inspectors should review records related to inspection, testing and calibration of security equipment and frequency of related actions to ensure that these are being conducted. Records available for review and consultation should include, but are not limited to, manufacturers maintenance recommendations, system plans or schematics, test records/logs, and deficiencies/system failures with repair documentation. Inspectors are encouraged ask the VSO questions related to inspection, testing, calibration, and maintenance of security equipment. Inspectors may also question the VSO and other personnel with security duties how the system (and subsystems) work, including a demonstration of system functionality and any appropriate tests/alerts. The inspector should issue a "no sail" requirement or COTP order after consulting the OCMI or COTP if a security system is inoperable. A system might mean one or more components that enable the equipment to perform the required service. The failure of one component on a large system that has back-up measures would not be as significant as the failure of a single component of a small system with no back-up. The inspector may consider other measures to mitigate risk if required to maintain acceptable security, or if requested by the operator to continue operations (e.g., a sentry in place of an intrusion alarm. If such alternative is required or requested, the overall effect on vessel operations and staffing levels must be considered.*

Security measures for access control.

33 CFR 104.265  
ISPS, Part A, 7.2.2  
ISPS, Part B, 9.9

*Inspectors may observe procedures in place to deter unauthorized access of people and the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports and whether security personnel show competence in these duties. Passenger vessels and ferries may comply with the measures contained in 33 CFR 104.292. Inspectors should cite the approved Security Plan and verify that the security measures specified for the current MARSEC level are in effect and deemed adequate. These measures include, but are not limited to, access points examined (gates, gangways, ramps, piers), identification procedures (personnel, vehicles, and vendors), and entry restrictions/prohibitions regarding access to the vessel (guards, fences, checkpoints, etc). In addition to the current MARSEC level, measures for other MARSEC levels should be examined. Inspectors should question VSOs and other personnel with security duties regarding additional security measures for elevations in MARSEC level requirements as specified in their specific Security Plan. This includes, but is not limited to: additional personnel, equipment, further limitations on access, and additional screening procedures. As an example, additional measures may include limiting the number of access points, deterring waterside access, suspending operations, and evacuation measures. The inspector should verify that the VSP addresses security measures for periods when the vessel is unattended, such as for daytime only operations. The inspector should issue a "no sail" requirement or COTP order after consulting the OCMI or COTP if the security measures for access control are grossly inadequate due to failure to comply with the VSP, or the VSP does not address the actual situation (e.g., the security personnel assigned can not*



control access because of the volume of persons attempting to enter).

Security measures for restricted areas.

33 CFR 104.270  
ISPS, Part A, 7.2.4  
ISPS, Part B, 9.18

*Inspectors may observe procedures in place to prevent and deter unauthorized access to those Restricted Areas identified in the Security Plan. These areas include, but are not limited to, storage and supply sites, shore areas immediately adjacent to each vessel moored at a facility, areas containing critical infrastructure/equipment (power, water, command/control, etc), and locations designed for loading cargo. Inspectors should cite the approved Security Plan and verify Restricted Area status for the current MARSEC level is in effect and deemed adequate. This includes, but is not limited to, the verification of locks or secured access points, locations properly marked and identified as Restricted Areas, surveillance equipment, and guards or patrols. Inspectors should question VSOs and other personnel with security duties regarding additional Restricted Area security measures for elevations in MARSEC level requirements as specified in their Security Plan. This includes, but is not limited to: additional personnel, equipment, further limitations on restricted areas, and additional surveillance procedures. Nothing in this section shall compromise the safety of the vessel, crew, or passengers (i.e., locks that block emergency escape scuttles). The inspector should issue a "no sail" requirement or COTP order after consulting the OCMI or COTP if the measures for controlling access to restricted areas leave these areas vulnerable with not means to mitigate the risk.*

Security measures for handling cargo.

33 CFR 104.275  
ISPS, Part A, 7.2.6  
ISPS, Part B, 9.25

*Inspectors may observe procedures in place to ensure the security of cargo handling operations and whether security personnel show competence in these duties. Inspectors should cite the approved Security Plan and verify Cargo Handling Security Procedures for the current MARSEC level are in effect and deemed adequate. These procedures include, but are not limited to, deterrence of cargo tampering, identification of unauthorized cargo (e.g., inventory control), and checking cargo for dangerous or unauthorized substances. In particular, a vessel's inventory procedures (logs, etc) should be examined to ensure all hazmat and CDCs are accurately tracked and accounted for. Inspectors should question VSOs and other personnel with security duties regarding additional cargo handling security measures for elevations in MARSEC level requirements as specified in their Security Plan. This includes, but is not limited to: increased screening of cargo and inventory, search of delivery vehicles, vehicle escort provisions, additional measures to prevent tampering (e.g., seals), and suspending operation.*

Security measures for delivery of vessel stores and bunkers.

33 CFR 104.280  
ISPS, Part A, 7.2.6  
ISPS, Part B, 9.33

*The security of vessel deliveries and bunkering operations must be in accordance with the VSP. Inspectors may observe procedures in place to ensure that security personnel demonstrate competence in these duties. Inspectors should cite the approved Security Plan and verify vessel delivery and bunkering procedures for the current MARSEC level are in effect and deemed adequate. These procedures include, but are not limited to; deterrence of tampering to stores, supplies and bunkers, identification of unauthorized deliveries (inventory control), and checking deliveries for dangerous or unauthorized substances. Inspectors should question VSOs and other personnel with security duties regarding additional vessel delivery and bunkering security measures for elevations in MARSEC level requirements as specified in their Security Plan. This includes, but is not limited to: increased screening of stores and inventory, search of delivery vehicles, vehicle escort provisions, additional measures to prevent tampering (seals), and suspending operations. Inspectors should determine how recurring and non-recurring deliveries are addressed in the Security Plan. The inspector should issue a "no sail" requirement or COTP order after consulting the OCMI or COTP if the security measures for delivery of vessel stores and bunkers are grossly inadequate to protect the vessel.*

Security measures for monitoring.

33 CFR 104.285  
ISPS, Part A, 7.2.5  
ISPS, Part B, 9.42

*The VSP may specify a variety of measures for monitoring. It is generally the practice to conduct vessel inspections during daylight hours, which might make determining if some measures are adequate (e.g., lighting). Some measures such as intrusion may be tested at any time. In any case, if the inspector is in doubt as to whether a measure is adequate, a demonstration may be necessary. The inspector should review the measures that are specified in the VSP and require performance testing of any measure that appears questionable.*

Security incident procedures.

33 CFR 104.290

*In verifying compliance with these sections, the individual performing the on-site inspection should confirm that the vessel has the equipment and/or personnel necessary to carryout the procedure as detailed in the security plan. For example, if the plan specifies that, in the event of a security incident, the VSO will notify authorities via radio, does the vessel have a radio that is capable of communicating with the appropriate authorities? Drill should incorporate security incidents procedures that are outlined in the plan.*

Additional requirements--passenger vessels and ferries.

33 CFR 104.292

*One important item that the inspector should keep in mind is the fact that the Vessel Security Plans were approved without anyone visiting the vessel. Therefore, if the inspector finds that the alternatives the vessel implemented do not provide the equivalent level of security provided by ID checks and screenings, the inspector should require the vessel owner to amend the VSP.*

Additional requirements--cruise ships.

33 CFR 104.295

*If the inspector finds areas of the plan that is not adequate or, not accurate (based on the configuration of the vessel, i.e. Vessel Security Plan quoted that the vessel did not have a radio room, but an onboard visit to the vessel found otherwise) the plan would need to be amended. Such cases may be common, since these plans were approved without on-site visits.*

Additional requirements--vessels on international voyages.

33 CFR 104.297  
ISPS, Part A, 19.1

*Prior to undertaking an international voyage the owner/operator of a vessel subject to SOLAS without a current ISSC will need to request an inspection from the local Officer in Charge Marine Inspection. After the inspection is completed, and the inspector finds that the provisions of Part 104 and the ISPS Code have been addressed, the vessel will receive an International Ship Security Certificate (ISSC), valid for a maximum of 5 years. An ISSC may not be issued unless a vessel is in full compliance, i.e., no deficiencies may be issued. An ISSC may be issued for less than 5 years in order that it may harmonize with the Certificate of Inspection or other international certificates.*

Assessment

33 CFR 104.300

*The inspector should consider whether the measures found in 33 CFR 104.300 (d) have been adequately addressed in the assessment during the verification. If one or more of these considerations do not appear to be addressed, the inspector should discuss it with the VSO or CSO as appropriate. The inspector may consider asking the name and qualifications of any third party expert consulted during the assessment.*

Amendment and Audit.

33 CFR 104.415

Amendments to VSP:

The VSP is a living document, able to change to incorporate changes or lessons learned. Local COTP's may initiate amendments, as well as conduct onsite verification of plan changes initiated by the facility/vessel owner or operator. VSP amendments should be tracked and recorded in the vessel file. To ensure amendments are consistent and meet regulatory intent, changes to plans will be reviewed and approved by MSC. For that reason, there are specific timeframes for amendments spelled out in the regulations.

Amendments to ASP

Should an enforcement inspection reveal that an owner/operator has correctly implemented an approved ASP in its entirety but security vulnerabilities exist in the vessel operation, the COTP shall be advised. Under 33 CFR 104.415 (a) (ii), the inspector can determine that an amendment is necessary and forward the recommendation through the chain of command to Commandant (G-MP). If deemed appropriate, (G-MP) will advise the organization that submitted the ASP for approval accordingly. Following such notification, it will be necessary for the original submitting organization to provide their proposed amendment to the Commandant (G-MP) for review and approval. If the submitting organization does not wish to amend the ASP, the vessel owner must submit a VSP for the vessel to the MSC. Amendments only include changes that are required or proposed to the plan template.

Audits:

*At a minimum, the regulations require the CSO, or VSO to ensure an annual audit is performed by personnel with knowledge in conducting audits and inspections, and control and monitoring techniques. The use of independent auditors is allowed. Vessels are also given flexibility in how they assign auditors depending on the unique nature and size of the company and vessels. Audits may also be required due to structure modifications on the vessel, or changes in operations, security measures, and response plans. Other vessel changes that impact the VSP may also trigger an audit. Audits may result in amendments to the overall VSP.*

*Nothing in the regulations prohibits the audit from being performed in conjunction with the scheduled security inspection conducted by the Coast Guard, as long as an audit is done at least every calendar year. However, the initial audit must be complete not more than one year from the VSP approval date. If a combined inspection/audit is performed, the inspector may review the qualifications of the auditor to ensure that the regulations for auditor's qualifications are met.*

Ship Security Alerts System

ISPS 9.4.18  
SOLAS XI-2, Reg 6

*The Ship Security Alert System (SSAS) is required only on vessels that are subject to SOLAS. The inspector should review the applicable requirements to determine when the vessel must comply. ISPS requires the VSP to contain information regarding the SSAS, but allows this section to be kept separate from the other sections to protect the details of its operation from compromise. The inspector should ask the VSO to examine this section and review the information. The inspector must take care to safeguard the location from unauthorized personnel, but should test it in accordance with the procedures found in the VSP. If the SSAS is part of the approved plan, the inspector should issue a "no sail" requirement or COTP order after consulting the OCMI or COTP if the SSAS is found inoperable, or is not covert.*

Glossary of Terms/Acronyms

**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.

**ALTERNATIVE SECURITY PROGRAM**

A third-party or industry organization developed standard that the Commandant has determined provides an equivalent level of security to that established by this subchapter.

**BARGE**

A non-self-propelled vessel (46 CFR 24.10-1)

**CERTAIN DANGEROUS CARGO (CDC)**

Means the same as defined in 33 CFR 160.203.

**CHARTERER**

Any person or entity that exercises operational control over a vessel subject to the requirements of this subchapter.

**CONTRACTING GOVERNMENT**

Any government of a nation that is a signatory to SOLAS.

**COTP**

Captain of the Port.

**CRUISE SHIP**

Any vessel over 100 gross register tons, carrying more than 12 passengers for hire which makes voyages lasting more than 24 hours, of which any part is on the high seas. Passengers from cruise ships are embarked or disembarked in the U.S. or its territories. Cruise ships do not include ferries that hold Coast Guard Certificates of Inspection endorsed for "Lakes, Bays, and Sounds", that transit international waters for only short periods of time on frequent schedules.

**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.

**DRILL**

A training event that tests at least one component of the AMS, vessel, or facility security plan and is used to maintain a high level of security readiness.

**EXERCISE**

A comprehensive training event involving several of the functional elements of the AMS, vessel, or facility security plan, and which tests communications, coordination, resource availability, and response.

**FERRY**

a vessel which is limited in its use to the carriage of deck passengers or vehicles or both, operates on a short run on a frequent schedule between two or more points over the most direct water route, other than in ocean or coastwise service.

**INTERNATIONAL MARITIME ORGANIZATION (IMO)**

A specialized agency of the United Nations concerned solely with maritime affairs and responsible for international treaties, conventions, resolutions and codes to improve Maritime safety.

#### ISPS CODE

The International Ship and Port Facility Security Code, as incorporated into SOLAS, is a set of security requirements for vessels subject on international voyages.

#### MARITIME SECURITY (MARSEC) DIRECTIVE

An instruction issued by the Commandant, or his/her delegate, mandating specific security measures for vessels and facilities that may be involved in a transportation security incident.

#### MASTER

The holder of a valid license that authorizes the individual to serve as a Master, operator, or person in charge of the rated vessel and who is serving in that capacity. For the purposes of this subchapter, Master also includes the Person in Charge of a MODU, and the operator of an uninspected towing vessel.

#### OWNER OR OPERATOR

Any person or entity that maintains operational control over a vessel subject to the requirements of this subchapter.

#### PASSENGER VESSEL

- (1) On an international voyage, a vessel carrying more than 12 passengers; and
- (2) On other than an international voyage:
  - (i) A vessel of at least 100 gross register tons carrying more than 12 passengers, including at least one passenger-for-hire;
  - (ii) A vessel of less than 100 gross register tons carrying more than 6 passengers, including at least one passenger-for-hire;
  - (iii) A vessel that is chartered and carrying more than 12 passengers;
  - (iv) A submersible vessel that is carrying at least one passenger-for-hire; or
  - (v) A wing-in-ground craft, regardless of tonnage, that is carrying at least one passenger-for-hire.

#### SAFETY OF LIFE AT SEA (SOLAS)

The International Convention for the Safety of Life at Sea sets certain safety requirements for vessels on an international voyage.

#### SECURITY SYSTEM

A device or multiple devices designed, installed and operated to monitor, detect, observe or communicate about activity that may pose a security threat in a location or locations on a vessel or facility.

#### STCW

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

#### VESSEL SECURITY ASSESSMENT (VSA)

An analysis that examines and evaluates the vessel and its operations taking into account possible threats, vulnerabilities, and existing protective measures, procedures and operations.

#### VESSEL SECURITY OFFICER (VSO)

The person onboard the vessel, accountable to the Master, designated by the Company as responsible for security of the vessel, including implementation and maintenance of the Vessel Security Plan, and for liaison with the Facility Security Officer and the vessel's Company Security Officer. (Also called SSO – Ship Security Officer)

#### VESSEL SECURITY PLAN (VSP)

The plan developed to ensure the application of security measures designed to protect the vessel and the facility that the vessel is servicing or interacting with, the vessel's cargoes, and persons on board at the respective MARSEC Levels.

#### VESSEL STORES

- (1) Materials that are on board a vessel for the upkeep, maintenance, safety, operation or navigation of the vessel; and
- (2) Materials for the safety or comfort of the vessel's passengers or crew, including any provisions for the vessel's passengers or crew.

**ENCLOSURE (8)**  
**ADDITIONAL POLICY GUIDANCE**

## **8.1. Additional Policy Guidance**

**8.2. Introduction:** Regulations mandated by MTSA and the ISPS Code place the responsibility of completing an accurate security assessment and addressing the vulnerabilities in the Vessel Security Plan or Ship Security Plan on the owner or operator of a vessel. The Coast Guard has the responsibility to review and approve the VSP and verify the vessel is complying with the approved plan. The following material is provided to supplement existing guidance in the preambles to the Interim Rule and the Final Rule, NVIC 04-03, and other policy guidance promulgated by the Coast Guard. As additional guidance continues to be developed, the MTSA-ISPS Helpdesk website (internet: <http://www.uscg.mil/hq/g-m/mp/MTSA.shtml>) should be checked regularly for the latest policy updates.

## **8.2 Plan Submission**

8.2.1 On 1 July 2004, any vessel that was operating prior to 31 December 2003, or that entered service prior to 30 June 2004, which is subject to the requirements of MTSA and/or ISPS and has not submitted a VSP or an ASP certification letter to the MSC will not be allowed to continue to operate in such a service. Such a vessel will be issued a COTP order directing it to cease operations. Appropriate civil penalty action must also be initiated.

8.2.2 New vessels (entering service on or after 1 July 2004) must submit their VSP 60 days prior to beginning MTSA and/or ISPS related operations.

8.2.3 Vessels subject to SOLAS on international voyages cannot use an ASP. However, several ASPs have been amended to include an international addendum. In these cases, a vessel may use the ASP base document but must submit a VSP to the MSC for approval. Since the ASP and addendum have been pre-approved, the review process should be expeditious.

8.2.4 Certain existing U.S. flagged vessels that may be subject to SOLAS Chapter XI-2 and ISPS because they occasionally sail on international voyages have implemented an approved ASP to cover domestic operations. Several of these vessels have indicated they will submit a VSP complying with the international requirements prior to sailing internationally. In those circumstances where a U.S. flagged vessel that complies with its MTSA requirements but does not meet ISPS the vessel should be issued a CG 835 prohibiting it from sailing on international voyages after 1 July 2004 and requiring it to submit its international VSP within 30 days. If the vessel decides it will no longer sail on international voyages and notifies the COTP in writing of this intention, the CG 835 will be rescinded.

## **8.3 Plan Review**

8.3.1 The U. S. Coast Guard Marine Safety Center is reviewing and approving all VSPs for U.S. flagged vessels subject to MTSA and ISPS, and those foreign flagged vessels subject to MTSA. In addition to approving VSPs, the Marine Safety Center is also reviewing and accepting letters submitted by owners or operators who are intending to implement an alternative security program (ASP).

8.3.2 It is the goal of the Coast Guard to review and approve all VSPs subject to MTSA prior to 1 July 2004. Because vessels subject to ISPS must have their VSPs approved prior to sailing on an

international voyage, these plans must be reviewed and approved as soon as possible. MTSA provides the Coast Guard with additional time to review and approve security plans for domestic vessels and facilities subject to MTSA. Therefore, the Marine Safety Center is reviewing plans in the following order:

- 1<sup>st</sup> priority: Vessels subject to ISPS intending to sail on international voyages.
- 2<sup>nd</sup> priority: Inspected vessels subject to MTSA that operate domestically, with a focus on passengers vessels subject to 46 CFR Subchapter H or K and vessels subject to 46 CFR Subchapters D or O.
- 3<sup>rd</sup> priority: Other inspected vessels and those uninspected vessels subject to MTSA.

8.3.3 Several improvements and modifications have been made to the Vessel Security Plan (VSP) review checklist. For the most recent version of the checklist and plan submittal guidance, please refer to the link provided on the MTSA/ISPS Help Desk website at <http://www.uscg.mil/hq/g-m/mp/MTSA.shtml> or at from the Marine Safety Center website at [http://www.uscg.mil/hq/msc/Security/sec\\_index.htm](http://www.uscg.mil/hq/msc/Security/sec_index.htm).

#### **8.4 Certificates And Verification Examinations For U.S. Flagged Vessels Subject To SOLAS Chapter XI-2 And ISPS**

8.4.1 Vessels subject to SOLAS Chapter XI-2, must be in compliance with the applicable requirements of SOLAS Chapter XI-1, SOLAS Chapter XI-2 and the ISPS Code, Part A and request an inspection for ISPS Code verification in accordance with 33 CFR 104.297

8.4.2 Generally, the Officer in Charge Marine Inspection (OCMI) would not complete the vessel security inspection and issue the ISSC until the VSP is approved by the Marine Safety Center. However, in order to streamline the process, the OCMI may issue an Interim ISSC after successfully completing the vessel security inspection confirming that the vessel has implemented its submitted VSP and meets all applicable security items in SOLAS Chapter XI-2 and the ISPS Code.

8.4.3 There are several benefits to issuing an Interim ISSC. The OCMI can spread out the verification inspections, providing additional flexibility in scheduling resources. The OCMI and the vessel may also combine the ISSC verification exam with other scheduled inspections, maximizing efficiency for both Coast Guard and vessel personnel associated with vessel inspections. The vessel may receive its inspection and Interim ISSC earlier, allowing it to commence an international voyage prior to VSP approval and later receive an ISSC without having a Coast Guard security inspector attend to the vessel in a foreign port. Significant amendments to the plan (i.e., anything more than administrative changes that do not affect procedures or equipment installations), between when the Interim ISSC is issued, and when the final plan approval is given, must then be reviewed by the ISSC issuance port prior to issuance of the permanent ISSC. If this amendment(s) is a hardware item, or a security device it may require a visit to the ship.

8.4.5 The Interim ISSC should be issued to expire on 30 June 2004, and the vessel must still receive its ISSC before 1 July 2004. Once the Interim ISSC is issued, the vessel must operate pursuant to the submitted VSP. The OCMI may subsequently administratively issue the ISSC once the Marine Safety Center approves the VSP without a second visit to the vessel, provided any deficiencies issued during the onboard verification examination have been corrected.



8.4.6 While an Interim ISSC may be issued based on a submitted plan and before the VSP is approved, no deficiencies can exist when the ISSC is issued. ISSCs must be dated prior to 1 July 2004 or the commencement of the international voyage, whichever is later. An ISSC that is issued to replace an Interim ISSC shall have the same date as the Interim ISSC. The expiration date of the ISSC may be up to five years but it may be issued for a shorter time period in order to harmonize it with the COI on inspected vessels or SOLAS documents on uninspected vessels.

8.4.7 An Interim ISSC is not the equivalent of a Temporary COI. If the vessel has an approved VSP and meets the requirements for an ISSC, an ISSC must be issued. Interim ISSCs must be issued only when necessary. A vessel may not receive consecutive Interim ISSCs.

## **8.5 Compliance Documentation For U.S. Flagged Vessels Operating Domestically**

8.5.1 On 1 July 2004, each U.S. flagged vessel subject to MTSA that operate domestically must have one of the following documents issued by the Marine Safety Center:

- Accepted ASP
- Approved VSP
- Interim Approval Letter
- Letter authorizing the vessel to continue to operate provided it remains in compliance with the submitted plan.

8.5.2 Effective 1 June 2004, the Commanding Officer of the MSC may issue an Interim Letter of Approval to a vessel that will by 1 July 2004 implement a VSP addressing the requirements of 33 CFR 104. Vessels that have passed Stage 1 of the VSP review process will generally be eligible to receive an interim approval letter. These interim approval letters will be issued with an expiration date of 31 October 2004.

8.5.3 Vessels that have incomplete VSPs will not receive interim approval letters allowing them to operate after 1 July 2004. COTPs will identify vessels in their fleet of responsibility that do not have an approved VSP, accepted ASP, or a VSP that has passed Stage 1. (note: the status of the VSP may be checked by viewing the G-MP Information site on the intranet. A vessel that indicates "Open - Security Plan Stage 1 Review" or "Open - Security Plan Stage 1 Returned For Revision" in the "status" column shall be issued a letter). COTPs will engage the owners or operators of these vessels to ensure they understand that they will be required to cease MTSA related operations after 30 June 2004 if, at a minimum, the VSP is not deemed to be complete. No later than 10 June 2004, COTPs will issue letters notifying the owners or operators of these vessels that they will be prohibited from performing MTSA related operations after 30 June 2004 unless they come into compliance. On 1 July 2004 COTPs will remove COIs (or reduce the operating limits, if applicable) of inspected vessels that do not possess one of the documents listed above. The sample letter (figure 8-1) may be used to notify vessel owners.

## Sample COTP Warning Letter

U.S. Department of  
Homeland Security

United States  
Coast Guard



June 10, 2004

Address

Dear Sir or Madam:

A review of our records indicates that you have submitted a Vessel Security Plan (VSP) to the Marine Safety Center in accordance with 33 CFR §104.410 for the vessel NAME (O.N. ). The plan that you submitted has not progressed beyond the first stage of review as of this date. Stage one is the first of three stages in the plan review process, and is the measure used to ensure that the VSP contains all required elements. A plan that does not pass the stage one review is missing some key element that must be in place in order to advance through the review process. Because your plan has not met this basic stage of review, it is ineligible to advance through the review process and will not be approved unless these problems are corrected.

Each vessel that is subject to 33 CFR §104 must be in compliance with an approved VSP on or before July 1, 2004. The plan that you have submitted will not meet this requirement, and you will not be authorized to engage in activities regulated by 33 CFR §104, beginning that date until this problem is corrected. This means that unless your VSP is revised and advances beyond stage one, your vessel's Certificate of Inspection may be removed or amended, or a Coast Guard requirement may be issued that prohibits your vessel from engaging in any regulated activities. Failure to comply with these restrictions may result in civil and/or criminal penalties against you. In addition, the vessel's crew may be subject to Suspension and Revocation action against any license or documents that they possess if found operating the vessel contrary to these restrictions.

To avoid these restrictions being placed on your vessel, you should contact the Marine Safety Center at (202) 366- 3879 or email at [securityplaninfo@msc.uscg.mil](mailto:securityplaninfo@msc.uscg.mil) immediately to discuss corrective actions that may be taken. If you are able to correct the problems with your VSP before July 1, 2004, but your plan remains unapproved, you may be eligible for a letter of authorization that will enable your vessel to continue to operate until final approval is achieved. Please contact me at ( ) ###-#### if you have any questions regarding the specific type of restrictions that may affect your vessel, or related matters.

Sincerely,

COTP

U.S. Coast Guard

Figure 8-1

8.5.4 Commandant (G-MP) is responsible for approving Alternative Security Programs (ASPs). Once approved, owners or operators of vessels may use an ASP if it is appropriate for that vessel. Owners or operators must submit a letter to the Marine Safety Center (MSC) stating the approved ASP the owner or operator will use.

8.5.5 Effective June 1, 2004, the MSC may issue a Letter of Authorization (LOA) to a Vessel to operate from July 1, 2004, until October 31, 2004. Vessel owner or operators that submitted a VSP, passed Stage I of the VSP review process, met any plan correction deadlines but still require

significant revisions to their VSP, will generally be eligible to receive a LOA. The MSC should identify those areas of the VSP that require significant revisions in the LOA. Furthermore, the LOA should stipulate that, in order for the Vessel to continue to operate on July 1, 2004, the owner or operator should develop and implement temporary measures to the satisfaction of the COTP in these areas. The following elements when deficient will normally be subject to temporary measures:

- Trained/qualified VSO
- Effective means of communication
- Sufficient security measures for access control
- Sufficient security measures for restricted areas
- Sufficient security measures for handling cargo
- Sufficient security measures for delivery of vessel stores/bunkers
- Sufficient security measures for monitoring
- Sufficient procedures for completing a DOS and performing the Vessel/vessel interface

8.5.6 In order to determine whether to issue a LOA, the MSC may review the current Stage II plan review letter or the Stage III checklist, as appropriate.

## **8.6 Enforcement Philosophy**

8.6.1 The three key steps of verification are to ensure the vessel complies with the VSP, ensure the completeness/accuracy of the Vessel Security Assessment (VSA) and ensure that measures are in place to adequately address vulnerabilities. The Coast Guard will work cooperatively with vessels while verifying compliance with their VSP, however vessels that require an ISSC must be in full compliance before the certificate can be issued. For those vessels on domestic only routes that are making a good faith effort to implement their VSPs and are in substantial compliance, on-the-spot corrections of minor deficiencies may be appropriate. For those vessels that are not in substantial compliance, progressive enforcement tools may be used, such as civil penalties and NOVs.

8.6.2 The COTP should consider the entire scale of enforcement tools available when issuing enforcement measures, such as documenting an initial, minor violation in a Letter or Warning, with subsequent violations documented in NOVs, civil penalties, or criminal penalties. The COTP must consult the cognizant District Legal Officer prior to initiating criminal penalty action.

8.6.3 Controls may also span the spectrum available to the COTP, such as restrictions on vessel operations documented on a CG 835 up to and including suspending operations and removing the COI from a vessel.

8.6.4 The compliance matrix below in figure 8-1 represents the criteria that the OCMI may use when determining what if any measures are required to ensure compliance. By finding the appropriate category for any deficiency and scoring the level of compliance, the recommended control or penalty action can be determined. A similar tool that contains the weighted scale for the various compliance levels that is for internal Coast Guard use only is located at <http://cgweb.comdt.uscg.mil/G-Mp/field.html>.

Enclosure (8) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 04-03

CATEGORY DESCRIPTION	RECOMMENDED CONTROL AND PENALTY MEASURES	
	FACILITY	VESSEL
	Severity of Deficiencies <i>Less Severe ----- &gt; More Severe</i>	Severity of Deficiencies <i>Less Severe ----- &gt; More Severe</i>
COMPLIANCE DOCUMENTATION	LAA, LOW, NOV, CP, OPC-4	LAA, LOW, NOV, CP, OPC-4
NON-COMPLIANCE	LAA, LOW, NOV	LAA, LOW, NOV
WAIVERS & EQUIVALENTS	LAA, LOW, NOV	LAA, LOW, NOV
MARSEC DIRECTIVES	AMD, LAA, LOW, NOV	AMD, LAA, LOW, NOV
MASTER KNOWLEDGE & TRAINING		LAA, LOW, NOV
CSO KNOWLEDGE & TRAINING		LAA, LOW, NOV
FSOVSO KNOWLEDGE & TRAINING	LAA, LOW, NOV, CP, OPC-4, OPC-5	LAA, LOW, NOV, CP, OPC-4, OPC-5
TRNG FOR PERSONNEL WITH SECURITY DUTIES	LAA, LOW, NOV	LAA, LOW, NOV
TRNG FOR PERSONNEL W/O SECURITY DUTIES	LAA, LOW, NOV	LAA, LOW, NOV
DRILL & EXERCISE REQUIREMENTS	AMD, LAA, LOW, NOV	AMD, LAA, LOW, NOV
RECORD KEEPING REQUIREMENTS	LAA, LOW, NOV	LAA, LOW, NOV
MARSEC LVL COORDINATION & IMPLEMENTATION	AMD, LAA, LOW, NOV	AMD, LAA, LOW, NOV
COMMUNICATIONS	AMD, LAA, LOW, NOV	AMD, LAA, LOW, NOV
DECLARATION OF SECURITY	LAA, LOW, NOV, CP, OPC-2	LAA, LOW, NOV, CP, OPC-2
SECURITY SYSTEMS EQUIP & MAINTENANCE	AMD, LAA, LOW, NOV	AMD, LAA, LOW, NOV
SECURITY MEASURES FOR ACCESS CONTROL	AMD, LAA, LOW, NOV, CP, OPC-1	AMD, LAA, LOW, NOV, CP, OPC-1
SECURITY MEASURES FOR RESTRICTED AREAS	AMD, LAA, LOW, NOV, CP, OPC-1	AMD, LAA, LOW, NOV, CP, OPC-1
SECURITY MEASURES FOR HANDLING CARGO	AMD, LAA, LOW, NOV, CP, OPC-2	AMD, LAA, LOW, NOV, CP, OPC-2
SECURITY MEASURES FOR STORES & BUNKERS	AMD, LAA, LOW, NOV, CP, OPC-2	AMD, LAA, LOW, NOV, CP, OPC-2
SECURITY MEASURES FOR MONITORING	AMD, LAA, LOW, NOV, CP, OPC-3	AMD, LAA, LOW, NOV, CP, OPC-3
SECURITY INCIDENT PROCEDURES	AMD, LAA	AMD, LAA
PASSENGER & FERRY FACILITIES ONLY	AMD, LAA, LOW, NOV, CP, OPC-3	
CRUISE SHIP TERMINALS ONLY	AMD, LAA, LOW, NOV, CP, OPC-3	
CDC FACILITIES ONLY	AMD, LAA, LOW, NOV, CP, OPC-3	
BARGE FLEETING FACILITIES ONLY	AMD, LAA, LOW, NOV, CP, OPC-3	
PASSENGER VLSL & FERRIES ONLY		AMD, LAA, LOW, NOV, CP, OPC-3
CRUISE SHIPS ONLY		AMD, LAA, LOW, NOV, CP, OPC-3

**CODES FOR CONTROL & COMPLIANCE MEASURES**

AMD - Require Plan Amendments (See 33 CFR 104.415 / 105.415)  
 LAA - Lesser Administrative Actions (e.g. Worklist/CG-835)  
 OPC - Operational Control Measures

- 1 - Restrictions on Access
- 2 - Restrictions on Cargo Ops
- 3 - Restrictions of Other Ops
- 4 - Suspension of MTSA / ISPS Operations
- 5 - Revocation or Suspension of plan

**CODES FOR PENALTY MEASURES**

LOW - Letter of Warning  
 NOV - Notice of Violation (Ticket)  
 CP - Civil Penalty

Figure 8-1

## **8.7 Enforcement Cycle And Control Actions For U.S. Flagged Vessels That Operate Domestically**

8.7.1 Unlike vessels subject to SOLAS Chapter XI-2 and ISPS, there is not a requirement to perform a verification examination onboard U.S. flagged vessels that operate domestically prior to the vessel operating.

8.7.2 From 1 July 2004 until 30 June 2005 the Coast Guard will verify that inspected vessels have implemented their approved security program. Thereafter, security program enforcement will be scheduled to coincide with the annual inspections. Any deficiencies noted during an intervening inspection must be addressed immediately.

8.7.3 Uninspected vessels must undergo verification, initially, at least once within the first two and one half years following July 1, 2004. After the initial verification, uninspected vessels must be verified at least twice every five years. The cognizant OCMI shall track the UTVs within their MTSA Fleet of Responsibility for the initial and subsequent verification exams. The OCMI shall contact the Company Security Officer to ensure that a verification is scheduled. A verification of the VSP may occur in connection with other Coast Guard boardings, such as post-casualty investigations if deemed appropriate by the investigator. All verifications must be entered into MISLE. An ISSC is required by the ISPS Code and will be issued for all vessels subject to SOLAS XI-2. Uninspected vessels are not required by regulation to have the VSP verified, however it is the Coast Guard's policy to conduct on board verifications and issue a boarding form as proof (see enclosure 3).

8.7.4 The COTP may verify vessel implementation on any vessel at any time, based on risk (e.g., high risk barge cargo in high consequence locations).

8.7.5 The COTP will conduct the initial and subsequent verifications using the CG 840 security book and document it in MISLE.

8.7.6 A Vessel Compliance Matrix has been completed that provides guidance for penalties, control efforts, etc (figure 8-1). Possible control actions include restricting or suspending vessel operations, etc. Control Actions may be may be conveyed using a variety of standard communications tools, based on the severity of the deficiency and associated control action, such as CG 835s for inspected vessels, Uninspected Towing Vessel Examination Reports for uninspected towing vessels, COTP orders, etc. The Vessel Compliance Matrix is aligned with the compliance checklist and identifies "show-stoppers". "Show-stoppers" are those deficiencies that may require the most stringent COTP control actions, such as suspension of operations.

8.7.7 Because a vessel operating under a Letter of Authorization must implement its submitted plan in its entirety, its compliance should be verified in the same fashion as a vessel with an approved plan.

8.7.8 When a vessel is in compliance with its VSP but the measures in the VSP (whether approved or awaiting approval) are not sufficient to reduce the identified vulnerabilities, the COTP should require the owner or operator to amend the plan. The COTP must do this in writing, and allow the

owner or operator at least 60 days to propose amendments. Until amendments are approved, the owner or operator shall ensure appropriate temporary security measures are implemented to the satisfaction of the COTP. Amendments must be submitted to the MSC for approval in accordance with 33 CFR 104.415. In these cases where the plan has been implemented but must be amended, no penalty action should be taken.

## **8.8 Suspending Operations**

8.8.1 If the COTP determines that a vessel must suspend operations, the COTP should issue a written COTP order directing the vessel to suspend 33 CFR 104 and/or ISPS regulated operations, as appropriate. For example, a vessel with an ISSC that does not have a valid CSR would not be allowed to perform ISPS regulated operations but could continue to operate domestically. If the violations are so egregious that the entire port is at risk, the COI should be revoked. The COTP may also suspend and revoke the VSP, thereby making the vessel ineligible to operate.

8.8.2 Controls may also span the spectrum available to the COTP, such as restrictions on vessel operations documented on a CG 835, issuing COI restrictions, as appropriate, up to and including suspending operations of the vessel using a COTP order and removing the COI from the vessel.

## **8.9 Intermittent Operations**

8.9.1 Many vessels perform MTSA regulated functions intermittently. A certificated vessel must implement its VSP at all times. For example, a passenger vessel certificated to carry more than 150 passengers must implement its VSP whenever it is carrying passengers, regardless of the number of passengers it is carrying. Once a vessel receives its ISSC or Interim ISSC, it must implement its approved VSP continuously. If a vessel with an ISSC or Interim ISSC ceases to implement its approved VSP the ISSC becomes invalid and the vessel must undergo a verification exam prior to resuming ISPS related operations.

8.9.2 However, an inspected vessel may have variable security measures for those periods when it is temporarily out of service, provided it is not carrying passengers or MTSA regulated cargoes. For example, a passenger vessel that is secured overnight may have minimal security measures in place while moored at its dock without passengers onboard. The VSA and VSP must address the variable security measures that the vessel will use, as well as those measures that it will use when resuming operations, such as sweeping the vessel after reestablishing access control.

8.9.3 An uninspected vessel may implement its plan continuously, or it may implement its plan only when performing MTSA regulated activities. The VSA and VSP must address the variable security measures that the vessel will use, as well as those measures that it will use when resuming operations, such as sweeping the vessel after reestablishing access control.

## **8.10 Declaration of Security (DoS) Applicability and Interfacing with Non-Compliant Foreign Ports**

8.10.1 Numerous questions have been received requesting a clarification of DoS applicability and use. The guidance below is provided to ensure consistency in the proper completion of the DoS.

- At MARSEC LEVEL 1: Only “cruise ship” (as defined by 33 CFR 101.105) and manned vessels carrying CDCs “in bulk” (as defined by 33 CFR 101.105) are required to complete a DOS, *if* there is a “vessel-to-vessel activity” or a “vessel-to-facility interface” (as defined by 33 CFR 101.105). However, if there are no actions that meet the definitions of “vessel-to-vessel activity” or a “vessel-to-facility interface”, then no DOS is required.
- At MARSEC LEVELS 2 and 3: All manned vessels to which 33 CFR Part 104 applies are required to complete a DOS, *if* there is a “vessel-to-vessel activity” or a “vessel-to-facility interface” (as defined by 33 CFR 101.105), this would include passenger barges, and uninspected towing vessels regardless of whether they are towing. However, if there are no actions that meet the definitions of “vessel-to-vessel activity” or a “vessel-to-facility interface”, then no DOS is required, i.e. if the vessel simply moors at the facility but there is no movement of persons, cargo, vessel stores or provisions of port services to or from the vessel no DOS is required. Dropping off or picking up a barge at a facility does not constitute a “vessel-to-facility interface”.
- At all MARSEC LEVELS: All unmanned vessels to which 33 CFR Part 104 applies are *not* required to complete a DOS. Other provisions of the regulations require owner and operators of unmanned barges to take into account the secure transfer of unmanned vessels from towing vessel to facilities. An unmanned barge remains unmanned regardless of tankermen or towing vessel crew working aboard the vessel.

8.10.2 The following “Declaration of Security (DoS) Applicability Decision Tool” (figure 8-2) provides a graphical representation for further delineating DoS applicability.

8.10.3 The MTSA regulations (33 CFR 104.250) were written with the expectation that a U.S. vessel is interfacing with an ISPS compliant foreign port. When a U.S. vessel is interfacing with a noncompliant ISPS port, the minimum following additional precautions would be considered adequate:

- a. MARSEC Level: In addition to the requirements outlined in 33 CFR 104.250, the Vessel Security Officer (VSO) sets MARSEC Level II unless information warrants an increase to MARSEC Level III.
- b. Declaration of Security (DoS): The VSO makes all attempts to coordinate security needs and procedures and agree upon the contents of the DoS with the noncompliant facility.
- c. Complete a Coast Guard questionnaire about the noncompliant port (to be available in the near future)

8.10.4 Upon the vessels return the COTP shall complete the following actions:

- a. MARSEC Level I: Conduct a MTSA compliance exam to ensure the crew is carrying out the provisions of its approved VSP. At a minimum the crew must be able to demonstrate their respective roles pertaining to the plan and courses of action they should take in order to mitigate security breaches.
- b. MARSEC Level II & III: Conduct a MTSA compliance exam offshore, similar to an ISPS I exam as outlined in NVIC 06-03.



### DECLARATION OF SECURITY (DoS) APPLICABILITY DECISION TOOL

This tool is designed to assist facility and vessel owners/operators in determining the need to execute a Declaration of Security (DoS) mandated by 33 CFR Parts 104 and 105.

**Step 1** – Utilizing Table 1, assign a category (CAT) for each vessel or facility involved in the interface<sup>1</sup>.

**TABLE 1 - VESSEL / FACILITY CATEGORY DECISION MATRIX**

Cruise Ship			A
33 CFR 104 Applicable Vessel / Barge	CDC <sup>2</sup>	Manned <sup>3</sup>	B
		Unmanned	C
	Non-CDC	Manned	D
		Unmanned	E
Not 33 CFR 104 Applicable Vessel / Barge	Manned		F
	Unmanned		G
33 CFR 105 Applicable Facility			H
Non 33 CFR 105 Applicable Facility			I
Barge Fleeting Facility			J

**Step 2** – Match the categories listed in Table 1 along the horizontal and vertical axes below in Table 2. It does not matter which axis is used. The appropriate (intersecting) cell indicates at which MARSEC Level a DoS would be appropriate. See Legend for further information.

**TABLE 2 – DOS INTERFACE DECISION MATRIX**

	A	B	C	D	E	F	G	H	I	J
A	1, 2, 3	1, 2, 3		1, 2, 3				1, 2, 3		
B	1, 2, 3	1, 2, 3		1, 2, 3				1, 2, 3		
C										
D	1, 2, 3	1, 2, 3		2, 3				2, 3		
E										
F										
G										
H	1, 2, 3	1, 2, 3		2, 3						
I										
J										

Table Legend

	No DoS Required
	DOS Required during identified MARSEC Levels
	Not Permitted by Regulations
	Not Applicable

Figure 8-2

<sup>1</sup> **Interface** means to engage in the transfer or movement of persons, cargo, stores, or provisions between a vessel and facility or a vessel and another vessel. See 33 CFR 101.105.

<sup>2</sup> Vessels are considered to be “CDC” if they are carrying cargoes listed in 33 CFR 160.204 “in bulk”.

<sup>3</sup> Vessels are considered “Manned” if a crew is required as per their Certificate of Inspection (COI). An unmanned barge remains “unmanned” regardless of Tankermen or towing vessel crew working aboard the vessel.

## **8.11 Statements of Voluntary Compliance (SOVC)**

8.11.1 Certain vessels that are owned or operated by the U. S. government request the Coast Guard to issue a SOVC in place of SOLAS Documents. While these vessels are generally not subject to port state control in foreign ports, the SOVC satisfies other requirements that make them desirable.

8.11.2 The Coast Guard or recognized classification society usually issues these documents through the normal inspection process. It is Coast Guard policy that any vessel that has received a SOVC for SOLAS certificates in the past will also receive an SOVC in place of the ISSC. A SOVC will also be issued in place of a Continuous Synopsis Record (CSR).

8.11.3 Because these vessels technically don't have to comply with SOLAS and are not subject to Port State Control, the SOVC will be forwarded to the vessel via the parent agency (i.e., Military Sealift Command, MARAD, etc.) once the Vessel Security Plan (VSP) is approved. The VSP of these vessels should be completed at the next scheduled inspection for Certification or annual exam after July 1, 2004. This inspection schedule will provide a similar level of compliance as is being applied to the U.S. flag domestic fleet that must comply with 33 CFR 104.

8.11.4 These vessels may be examined prior to the first scheduled exam at the convenience of the OCMI, if other opportunity presents itself (i.e., the verification may take place in concert with other inspections scheduled in the port).

8.11.5 Vessels enrolled in the Alternative Compliance Program must have the verification completed by a Coast Guard inspector.

## **8.12 Continuous Synopsis Record (CSR)**

8.12.1 Every vessel that is required to possess a valid ISSC must also carry a valid CSR. Some confusion has resulted from a misunderstanding of the relationship between the CSR and ISSC. A vessel must first obtain an ISSC, before receiving the CSR.

8.12.2 The CSR application process is outlined in Federal Register 9207, February 27, 2004. The owner/operator of a vessel subject to SOLAS must submit to the National Vessel Documentation Center (NVDC) the application form (CG-6039). The NVDC is the issuing authority for CSR on U.S. flag vessels. The CSR desk may be contacted at 1-866-603-5476

8.12.3 In order to meet the short turn-around time imposed by the initial deadline of July 1, 2004, the NVDC will make a scanned image of the CSR available in MISLE for the initial issue. This will occur when an application is received, but a record of an ISSC being issued does not exist in MISLE. The unit conducting the first issuance of a CSR should ask the owner/operator if a CSR application has been submitted and check the documents in MISLE before attending the vessel. If a CSR image is in MISLE the inspector may print a copy and emboss the certificate with the Coast Guard seal. The CSR may then be issued only if the ISSC is issued. This procedure will not normally occur after initial CSR issue.

### 8.13 Ship Identification Number (SIN)

8.13.1 Numerous questions have fielded regarding the requirement for the Ship Identification Number (SIN), *also known as the IMO number*. Although the SIN is not an ISPS requirement, it is a new SOLAS requirement that is often associated with the ISPS Code. The following guidance may be applied when verifying compliance with the SIN requirements:

- a. SOLAS XI-1/3.4 requires a vessel's IMO number to be permanently marked on the vessel. For U.S. flag vessels the number should be affixed to the vessel in a manner similar to that used to mark the vessels Official Number. The letters and numerals must be welded, cut or punched into a permanent structure on the vessel. Attaching a placard or plate to the structure of the vessel is not acceptable because removal or replacement of the number would not be apparent.
- b. Vessels that currently do not have an IMO number may obtain through Lloyds Register. More information may be obtained by visiting the Lloyds Register website at [www.lrfairplay.com/archway/Services/imonumber/imonetform.htm](http://www.lrfairplay.com/archway/Services/imonumber/imonetform.htm). Certain vessels are ineligible for an IMO number. Vessels less than 100 GT and vessels that belong to the U.S. government are exempt from the requirement to display the SIN as required.

### 8.14 Checking Identification and Performing Passenger, Baggage, Vehicle Screening

8.14.1 The MTSA regulations at 33 CFR 104.292 provide an alternative to the identification check and passenger screening requirements for passenger vessels and ferries. These measures include searching selected areas prior to embarking passengers and prior to sailing, and any of the following:

- a. Performing routine security patrols;
- b. Providing additional closed circuit television to monitor passenger areas; or
- c. Securing all non-passenger areas.

8.14.2 Any vessel owner/operator may use the alternative measures of 33 CFR 104.292 in their VSP or Alternative Security Program (ASP). The American Gaming Association and the Passenger Vessel Association ASPs are examples of two that have implemented measures that comply with 104.292.

8.14.3 Vessels that have implemented the alternative measures of 33 CFR 104.292 in their VSP or ASP are not required to check the identification of passengers or screen passengers, baggage, or personal effects at the rate specified in the applicable MARSEC Directives. However, because these alternatives replace the requirement for screening and the applicable MARSEC Directive, a vessel not in compliance with this portion of the plan may be subject to the penalties contained in 33 CFR 101.415.

8.14.3 At this time there is no alternative for vehicle screening. All passenger vessels and ferries carrying vehicles must screen those vehicles at the rate specified in the applicable MARSEC Directive.

8.14.4 The alternatives allowed under 33 CFR 104.292 encompass only the requirement to screen passengers and the applicable MARSEC Directives. MARSEC Directives that may be issued in the future, which govern other aspects of passenger vessel or ferry operations are not affected by the alternative measures of 104.292. Passenger vessels and ferries must comply with all MARSEC Directives except those that set specific passenger screening rates.

Enclosure (9) to NAVIGATION AND VESSEL INSPECTION CIRCULAR No. 04-03

**ENCLOSURE 9**

**GUIDANCE FOR CONDUCTING SECURITY AUDITS**

ENCLOSURE 9  
VESSEL SECURITY AUDITS

1. Title 33, Part 101.105 (33 CFR 101.105) defines *audit* as “an evaluation of a security assessment or security plan performed by an owner or operator, the owner or operator’s designee, or an approved third party, ***intended to identify deficiencies, non-conformities, and/or inadequacies that would render the assessment or plan insufficient.***” 33 CFR 104.415, 105.415, and 106.415 provide requirements for the conduct of an annual audit of a regulated facility or vessel security plan.
2. The intent of the regulation and the purpose of an audit are to identify opportunities for improvement and to address nonconformities. The audit accomplishes this through the review of the operations of the regulated entity and the implementation of corrective actions which ensure regulatory compliance and preclude the recurrence of deficiencies. If, during the course of an audit, deficiencies and/or inadequacies are identified, then the security assessment and security plan of the regulated entity could have areas requiring improvement or revision. In this continuation of the audit and review of the security plans and assessments, more than one fix may need to be made. For instance, an identified security gap allowing unaccounted for persons to access a regulated entity would indicate a possible nonconformity in the implementation of the plan, or possibly point to deficiencies in the plan and assessment. It is the intent of the audit to make the security posture, and the underlying documentation, align and provide the tightest security appropriate for the situation.
3. Several opportunities exist for the auditor to analyze the effectiveness of the regulated entity in implementing their security plan. For example, review of quarterly drills, annual exercises, and corrective action following a deficiency or recorded security event (such as security incidents or breaches of security) provide an auditor the chance to see the plan operate and learn how it has been improved. An effective audit might include site visits during normal and other-than-normal hours, interviews with and observation of personnel performing security duties, review of and observation of security procedure implementation, as well verifying operability testing and planned maintenance of security equipment and ensuring that personnel are trained and proficient in their security duties.
4. During the audit, several documents could assist the auditor in his or her duties. Such documents include those associated with previously performed audits, drills, exercises, security incidents, compliance inspections, corrective action reports, and lessons learned.
5. 33 CFR 104.235(b)(8) requires a letter certified by the Company Security Officer or the Vessel Security Officer stating the date the audit was completed. While there is no requirement that an audit report be maintained, the sample audit report form on the next page of this NVIC may be used by an auditor to help organize their thoughts and their findings.

**SAMPLE AUDIT REPORT FORM**

**NAME OF REGULATED ENTITY:**

**REPORT NUMBER:**

**AUDIT DATE(S):**

**DATE OF LAST AUDIT:**

**AUDITORS AND EVIDENCE THEY MEET 33 CFR 104.415(b)(4):**

- 1.)
- 2.)
- 3.)
- 4.)
- 5.)

**EXECUTIVE SUMMARY:**

*This section gives the auditor the opportunity to briefly describe their findings. Note: Requirements for the classification and protection of Sensitive Security Information is found in 49 CFR Part 1520.*

**DEFICIENCIES (D), NON-CONFORMITIES (N/C), PLAN INADEQUACIES (PI), OR AREAS FOR IMPROVEMENT (AFI) IDENTIFIED:**

- 1.)
- 2.)
- 3.)
- 4.)
- 5.)

**CURRENT SECURITY POSTURE:**

*This section gives the auditor the opportunity to describe Noteworthy Findings (NF), Observations (O), and Strengths (S).*

**NAME OF INVOLVED PARTIES FROM THE REGULATED ENTITY:**

- 1.)
- 2.)
- 3.)

Audit Report Prepared by: \_\_\_\_\_ Company: \_\_\_\_\_ Date: \_\_\_\_\_

Audit Report Reviewed by: \_\_\_\_\_ Position: \_\_\_\_\_ Date: \_\_\_\_\_

Audit Certification Letter Attached to VSP by: \_\_\_\_\_ Date: \_\_\_\_\_