U.S. Department of Homeland Security
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street SW
Washington, DC 20593-0001
Staff Symbol: CG-543
Phone: 202-372-1224
Facsimile: 202-372-1918
fldr-g-pcv@comdt.uscg.mil

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 HOMEPORT 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

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 MTSA/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.

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)

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

Enclosure (2) 33 CFR 104: General Policy Discussion

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

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

Enclosure (8) Additional Policy Guidance

Enclosure (9) Guidance for Conducting Security Audits

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 that 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 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. <u>Company Security Officer (CSO).</u> 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. <u>Vessel Security Officer (VSO).</u> 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. <u>Company and Vessel Personnel with Security Duties.</u> 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. <u>Vessel Record Keeping Requirements.</u> 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 (<u>Note</u>: 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. <u>Maritime Security (MARSEC) Level Coordination and Implementation.</u>
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/alarms.

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. <u>Security Measures for Handling Cargo.</u> 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. <u>Security Measures for Delivery of Vessel Stores and Bunkers.</u> 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. <u>Additional Requirements--Vessels on International Voyages.</u> 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. <u>Assessment .</u> 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. <u>Vessel Security Plan.</u> 33 CFR 104.400

33 CFR 104.400(a)(1) requires that the VSP identify of the CSO and VSO by name <u>or</u> 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. <u>Amendment and Audit.</u> 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.