U.S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-MOC-2
Phone: (202) 267-0495
Fax: (202) 267-0506
Email: fldr-g-moc@comdt.uscg.mil

COMDTPUB P16700.4
NVIC **05 03**

15 DECEMBER 2003

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 05 03

Subj: IMPLEMENTATION GUIDANCE FOR THE MARITIME SECURITY REGULATONS MANDATED BY THE MARITIME TRANSPORTATION SECURITY ACT OF 2002 FOR OUTER CONTINENTAL SHELF FACILITIES

Ref: (a) 33 CFR Part 106 (MARITIME SECURITY: OUTER CONTINENTAL SHELF FACILITIES)
(b) 33 CFR Part 104 (MARITIME SECURITY: VESSELS)

1. PURPOSE. This Navigation and Vessel Inspection Circular (NVIC) introduces guidelines for the implementation of the maritime security regulations mandated by the Maritime Transportation Security Act of 2002. The guidance contained herein details the plan review process and is intended to assist inspectors in the performance of their duties while conducting security examinations. This guidance is also intended for owners and operators of affected outer continental shelf (OCS) facilities as an aid for complying with reference (a).

2. ACTION.

a. Captains of the Port (COTP) and Officers in Charge, Marine Inspection (OCMI) are encuraged to bring this circular to the attention of marine interests within their areas of responsibility. This circular will be distributed by electronic means only. It is available on the World Wide Web through http://www.uscg.mil/hq/g-m/nvic/index00.htm.

b. OCS facility owners and operators may use this circular as guidance during verification and compliance inspections. These guidelines may be applied to verify compliance with the Facility Security Plans (FSP) and during drills or exercises conducted to ensure crew competency.

DISTRIBUTION SDL NO. 05 03 140

	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																										

3. DIRECTIVES AFFECTED. No current directives are affected.

4. BACKGROUND.

a. The purpose of the maritime security regulations found in the Code of Federal Regulations (CFR) Part 106 of Title 33 is to require security measures for OCS facilities in order to reduce the risk and mitigate the results of an act that threatens the security of personnel, the OCS facility, the environment, and the public. The Coast Guard is responsible for verifying that each affected OCS facility complies with the maritime security regulations.

b. 33 CFR Part 106 requires the owner or operator of each affected OCS facility to comply with an approved FSP or Alternative Security Program (ASP). Due to the variety of facility types to which these requirements apply, the methods used in the security plan to reach compliance may vary. It is important to recognize that OCS facilities have unique characteristics unto themselves and, as a result, varying security needs.

5. DISCUSSION.

a. This circular is designed to provide guidance to both Coast Guard and industry personnel on all aspects of the implementation policies for OCS facilities. Mobile Offshore Drilling Units (MODUs) that are not specifically regulated under reference (a) may be required to meet Reference (b) and the vessel security NVIC. See Enclosure (1) for applicability guidance.

b. From this point forward, “facility” or “OCS facility” will be used as a generic term for all facilities that meet the applicability requirements, including MODUs. Where necessary to specifically address the unique issues of MODUs, they will be specifically referenced as such.

c. The Coast Guard does, and will continue to, work with the Minerals Management Service in the area of compliance enforcement on the OCS.

6. IMPLEMENTATION.

- Enclosure (1) is an expanded discussion on the applicability of the security regulations for OCS facilities.
- Enclosure (2) is a flowchart, which guides the user through the FSP submission, review, and validation process.
- Enclosure (3) is an overview of the implementation & submission process.
- Enclosure (4) is a checklist for the Stage I general review of the OCS facility FSP.
- Enclosure (5) is a checklist for the Stage II detailed review of the OCS facility FSP.
- Enclosure (6) is a checklist for the Compliance Verification inspection performed by the COTP.

- Enclosure (7) contains sample letters from the USCG unit to OCS owners and operators.
- Enclosure (8) contains guidance for submission of Alternative Security Program (ASP)

7. INFORMATION SECURITY.

a. Security Assessments, security plans and their amendments contain information that, if released to the general public, would compromise the safety or security of the port and its users. This information is known as sensitive security information (SSI) and the Transportation Security Administration's (TSA) regulations that govern SSI are found in 49 CFR Part 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 Part 1520 for the marking, storing, distributing and destroying of SSI material, which also 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 Part 1520.11, will have access to security plans and assessments. Vessel and facility 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, in almost all circumstances, SSI material will not to be disclosed under the Freedom of Information Act.

c. When SSI is released to unauthorized persons, a report must be filed with the Department of Homeland Security. Such unauthorized release is grounds for a civil penalty and other enforcement or corrective action.

8. DISCLAIMER. While the guidance contained in this document may assist the industry, the public, the Coast Guard, and other Federal and State regulators in applying statutory and regulatory requirements, this guidance is not a substitute for applicable legal requirements, nor is it in itself a rule. Thus, it is not intended to, nor does it impose, legally binding requirements on any party, including the Coast Guard, other Federal agencies, the States, or the regulated community.

9. 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 ALDIST/ALCOAST, and posted in the website for the benefit of industry pending their inclusion to the next change to this circular. Suggestions for improvement of this circular should be submitted in writing to Commandant (G-MOC).

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

Encl:
(1) Applicability Discussion
(2) OCS Facilities Plan Review Process Methodology Flowchart
(3) Plan Review Guidelines and Implementation Policies
(4) Stage I (Preliminary Review) Guidance
(5) Stage II (Detailed FSP Review) Guidance
(6) Compliance Verification Procedures
(7) Sample Correspondence
(8) Guidance for Submission of Alternative Security Program (ASP)

Table of Contents

Implementation Guidance for the Maritime Security Regulations Mandated by the Maritime Transportation Security Act of 2002 For Outer Continental Shelf Facilities

Table of Contents

Applicability Discussion

1 Applicability Discussion

This section is intended to clarify the applicability of security regulations in 33 CFR 106 to OCS facilities of the United States. Many types of fixed and floating facilities and vessels are located on the OCS. The unique operations of individual OCS facilities will dictate whether the security regulations apply during certain times. This section will discuss applicability of 33 CFR 106 to the more common OCS facility types and their operations. Applicability is based on one or more of the following criteria:

- Number of personnel
- Amount of production
- OCS facility type

1.1 Personnel Standard

33 CFR 106.105(a) specifies the personnel standard for applicability as follows:

> (a) Hosts more than 150 persons for 12 hours or more in each 24-hour period continuously for 30 days or more.

Facilities may be capable of berthing more than 150 persons through permanent or temporary means, but may not actually exceed these levels during normal operations. Therefore, the applicability of this section cannot be determined by the potential capacity of an OCS facility. Facility owners or operators are accountable for determining if their facilities will exceed the manning standards.

A facility that normally operates below this threshold, but later determines a need to exceed it for an anticipated operation, should forward an updated FSP to the CG District Commander 60 days prior to the commencement of the operations. The owner or operator may submit a request for waiver of the 60-day advance notice to the CG District Commander, but only for exceptional circumstances.

If manning declines below this threshold, and the facility no longer desires to operate under its security plan, the facility should notify the cognizant CG District Commander. The company should provide the reason(s) the regulations are no longer applicable (e.g. a drop in manning due to removal of a drilling crew, abandoning of a facility.) If there is reasonable chance of increasing above those thresholds again in the near future, requests to drop compliance for short durations will not normally be accepted. Compliance with the existing FSP should continue until the cognizant CG District Commander has approved the request. Should manning levels rise again, the facility will need to resubmit an FSP in accordance with 33 CFR 106.

Facilities that are linked together by walkways allowing movement of personnel between individual platforms will be considered one OCS facility. To determine if personnel thresholds have been exceeded, the number of persons on each linked platform should be totaled. This includes elevating vessels that work alongside a fixed structure. For example, the additional personnel on MODU or liftboat temporarily connected to a facility for drilling, work-over, or other operations are to be considered in the total number for applicability purposes.

1.2 Production Standards

33 CFR 106.105(b) and (c) specifies the production standards at a facility that should comply with part 106 as follows:

(b) Produces greater than 100,000 barrels of oil per day; or

(c) Produces greater than 200 million cubic feet of natural gas per day.

For the purposes of part 106, production is defined the same as it is in 33 CFR 140.10:

> *Production means those activities which take place after the successful completion of any means for the removal of minerals, including, but not limited to, such removal, field operations, transfer of minerals to shore, operation monitoring, maintenance, and workover.*

As noted, production includes the statement; "transfer of minerals to shore," that encompasses fixed facilities that operate as "Transmission Facilities." Production quantities shall be calculated as the sum of all sources of production from wells on the primary and any attending platform(s), including the throughput of other pipelines transferring product across the same platform(s).

Existing facilities should use their past, one-year production average(s) to determine applicability of these regulations. Existing facilities that did not originally exceed this average, but anticipate exceeding these thresholds in the future, should submit an FSP (as per encl. 3) 60 days prior to the anticipated date that the production will exceed the threshold requirement(s).

Applicability of the regulation to a new facility will be based on the designed or anticipated production levels. Validation of the applicability may occur no sooner than one year following commencement of operations.

If the average level of production falls below the threshold(s) over one year and the OCS facility no longer plans to operate under its approved FSP, the owner or operator should notify the cognizant CG District Commander and request an exemption from compliance with 33 CFR 106. The letter should state the reason for the request. Compliance with 33 CFR 106 should continue until the cognizant CG District Commander has approved the request. If production levels rise again, the facility will need to submit a new FSP in accordance with 33 CFR 106 and this NVIC.

1.3 OCS Facility Type Guidelines

OCS activities use many different types of vessels and facilities. To eliminate potential confusion, the most common types of vessels and facilities are discussed as related to applicability of security regulations.

1.3.1 Fixed OCS Facilities (Platforms)

The definition of an OCS facility in 33 CFR 106 includes fixed OCS facilities as defined in 33 CFR 140.10 that meet the threshold values outlined in 33 CFR 106.105.

> *Fixed OCS facility is defined as a bottom founded OCS facility permanently attached to the seabed or subsoil of the OCS, including platforms, guyed towers, articulated gravity platforms and other structures.*

Platforms that are connected together with catwalks should be considered as one for the purposes of applicability.

1.3.2 Transmission Platforms

Transmission facilities are those facilities whose primary purpose is the pumping, maintenance, and/or inspection of transfer pipelines. Transmission facilities are required to comply with the requirements of 33 CFR 106.

A forthcoming Notice of Policy will be published in the Federal Register to further explain the applicability of these security regulations to transmission platforms.

1.3.3 MODUs

As per 33 CFR 104.105(a)(1), MODUs that are subject to the International Convention for the Safety of Life at Sea, 1974 (SOLAS), Chapter XI-2 are subject to the provisions of 33 CFR 104. MODUs that are not subject to SOLAS, but exceed the personnel criteria of 33 CFR 106.105(a), are required to comply with provisions of 33 CFR 106.

A foreign flagged MODU operating on the OCS with a Letter of Compliance issued under 33 CFR 143.210 is still required to operate in compliance with the ISPS Code, provided it meets the applicability requirements. Further details can be found in the U.S. Vessel Maritime Security NVIC. If the ISPS Code does not apply, the MODU may be subject to the requirements of 33 CFR 106.

MODUs are generally employed for exploratory, production, and work-over drilling. They are not involved with production of oil and gas, and under most cases should not be compared against the production criteria of 33 CFR 106.105(b) & (c).

1.3.4 Tender Assisted Drilling Rigs

Personnel on vessels required for the purposes of providing assistance on a drilling rig should be included in determining application with personnel thresholds in 33 CFR 106.

1.3.5 Floating OCS Facilities

An OCS facility includes floating OCS facilities as defined in 33 CFR 140.10 that meet the threshold values outlined in 33 CFR 106.105.

> *Floating OCS facility means a buoyant OCS facility securely and substantially moored so that it cannot be moved without a special effort. This term includes Tension Leg Platforms (TLP) and permanently moored semi-submersibles or shipshape hulls, but does not include mobile offshore drilling units or other vessels.*

This category would also include Spars and variations of Spars and TLPs and any other similar type floating OCS facility that might develop in the future.

1.3.6 Floating Production Storage and Offloading (FPSO)

FPSOs that are operating in the U.S. OCS are subject to the rules in 33 CFR 106 if they exceed any of the thresholds outlined in 33 CFR 106.105. Although FPSOs are classified as vessels, due to the nature of their operations, they are best suited for coverage by 33 CFR 106 and will be considered as facilities only for the purpose of compliance with the maritime security regulations.

1.3.7 Other Operations

Operations on the U.S. OCS have been marked with constantly developing, unique, and novel vessels and facilities that do not often fit into the current regulatory structure. When additional, unique facilities are developed for operations in the U.S. OCS, the company may request a determination of applicability from the cognizant CG District Commander.

Table 1-1: Facility Types and Their Applicability

Facility Type	Applicability
Fixed Production Platforms	33 CFR 106 (OCS Facilities)
Fixed Transmission Platforms	33 CFR 106 (OCS Facilities)
FPSOs	33 CFR 106 (OCS Facilities)
Liftboats (Most operations)	33 CFR 104 (Vessels)
Liftboats (Elevated operations >30 days & >150 persons)	33 CFR 106 (OCS Facilities)
MODUs (SOLAS)	33 CFR 104 (Vessels)
MODUs (Non-SOLAS)	33 CFR 106 (OCS Facilities)
Deepwater Ports	33 CFR Subchapter NN (Deepwater Ports)
Floating OCS Facilities	33 CFR 106 (OCS Facilities)
TLPs / Spars	33 CFR 106 (OCS Facilities)

2 Operational Impacts on Applicability

MODU operations can change in ways that affect an approved FSP. The following discussion details common operational events and their effects upon compliance with this regulation. While the examples focus on changes in MODUs operations that exceed personnel thresholds of this

regulation, floating facilities, such as Spars, TLPs, and FPSOs can experience similar changes at their locations. When these changes occur, all types of facilities should follow the basic procedures for MODUs outlined in this section.

A facility may cease operating in compliance with its FSP upon conclusion of drilling or production operations and notification. The owner or operator should inform the cognizant CG District Commander of the intent to cease operations in anticipation of a facility move. The CG District Commander is not required to respond to this notice.

For purposes of this regulation, facilities engaging in the exploration, development, or production of oil, natural gas, or mineral resources that are regulated by 33 CFR subchapter N are required to operate in compliance with its approved FSP. For a new production facility, the applicability of these regulations commences upon perforation of a well.

A MODU is only required to comply with its approved FSP while on location on the OCS.

2.1 Facilities Changing Operations Between Coast Guard Districts

Occasionally, facilities may move operations between Coast Guard District AORs. If a move occurs, the facility does not need to resubmit an FSP, but the owner or operator should notify both CG District Commanders of the intended move. The facility will be required to submit the following items to the gaining CG District Commander 60 days prior to the initiation of operations in the new location:

- Approved FSP with previous amendments
- Previous Approval Letter from the CG District Commander at the MODU's former location of operation
- Request for approval of an amendment that considers changes to the facilities operation

The gaining CG District Commander has the authority to require a new FSP if security concerns of the new operation are determined to be notably different.

2.2 Facilities Changing Locations within a Coast Guard District

Facilities, particularly MODUs, commonly change operations within a single Coast Guard District AOR. The owner or operator should notify the cognizant CG District Commander of the intended move. While the facility will not be required to submit a new FSP, the plan is specific to a location, so any move will require an amendment. When a facility plans to change its operational location, it should submit an amendment request to the cognizant CG District Commander 60 days prior to the initiation of operations in the new location.

If the relocation includes movement to another COTP zone, a copy of the approved FSP with amendments (written & electronic) will be submitted along with the request for amendment. The CG District Commander will forward this copy to the gaining cognizant COTP.

The CG District Commander has the authority to require a new FSP if that security concerns of the new operation are determined to be notably different.

2.3 Facilities Departing U.S. OCS for Foreign Service or Taken Out of Service

Facilities moving off location into lay-up status or to foreign, overseas locations should notify the cognizant CG District Commander as discussed in the beginning of this section. Enforcement of the FSP will cease upon conclusion of production or exploration operations in anticipation of the pending movement.

2.4 Return of Facilities from Foreign Service or Lay-up – Previously Approved FSP

When a facility, which previously operated in the U.S. OCS under a previously approved FSP, returns to U.S. OCS service, it should notify the cognizant CG District Commander. The facility may not be required to resubmit an FSP, but an FSP approval letter from the gaining CG District Commander for the expected change of location of operations will need to be re-issued.

The facility should submit the following items to the gaining CG District Commander 30 days prior to the initiation of operations in the new location:

- Approved FSP with previous amendments
- Previous Approval Letter from the CG District Commander in which the MODU formerly operated
- Request for approval of an amendment that considers changes to the facility's operation
- Most recent notification of cessation of operations

Once reviewed and approved, the CG District Commander will issue a new FSP Approval Letter to the facility. This letter should be aligned to expire at the same 5-year interval as the previous approval letter, if it has not expired. Otherwise, the new Approval Letter will be issued to expire in 5 years. The issued Approval Letter should refer to the acceptance of the amendments to the plan. No individual Amendment Approval Letter is necessary. The CG District Commander will forward a copy of the FSP to the gaining cognizant COTP.

The CG District Commander has the authority to require a new FSP if security concerns of the new operation are determined to be notably different.

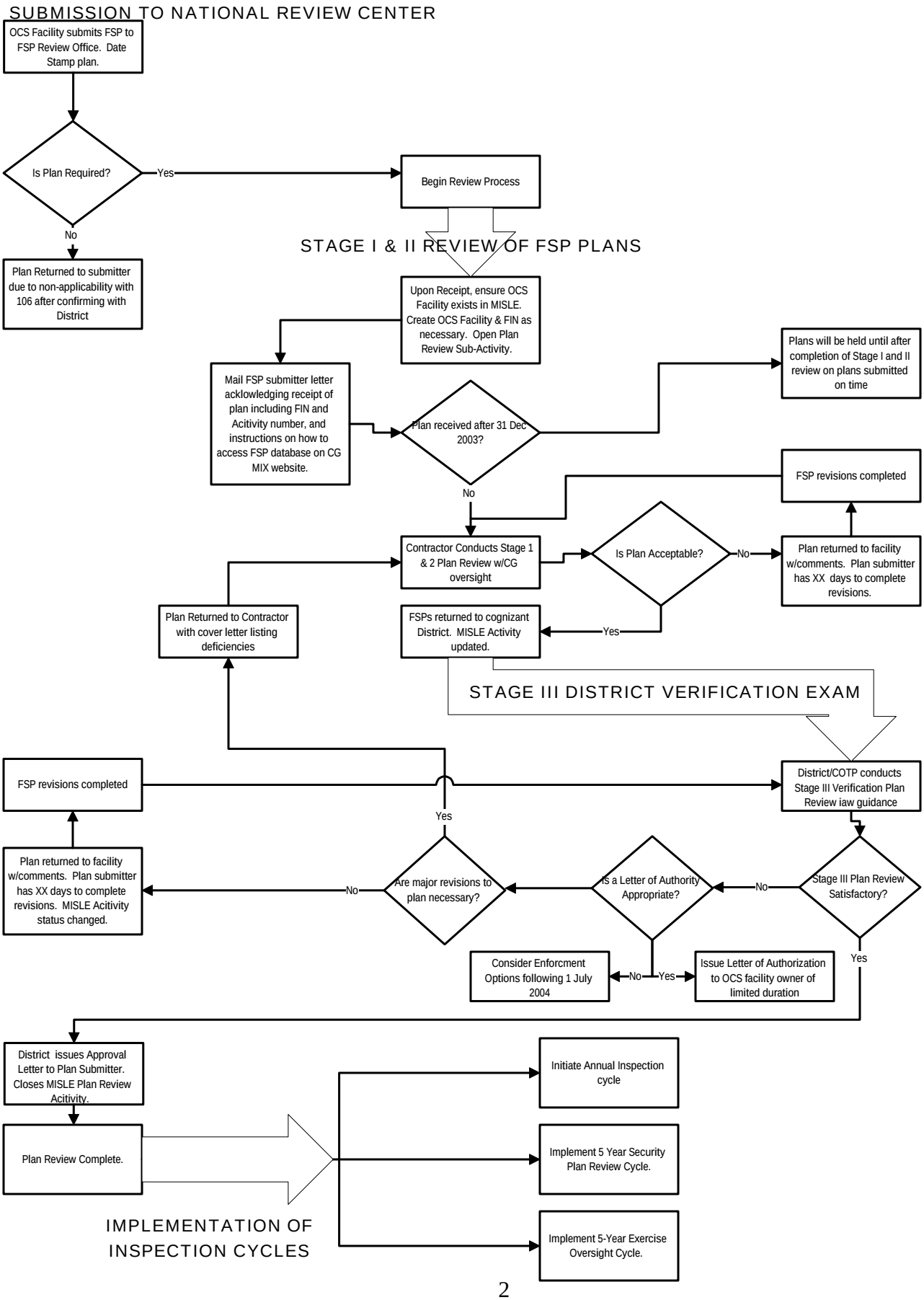
2.5 New Facility or Foreign Facility Entering the U.S. OCS – No Previous FSP

New facilities or foreign facilities entering the U.S. OCS that have not had a previous FSP should submit an FSP to the cognizant CG District Commander 60 days prior to the initiation of operations. Procedures will be in accordance with Enclosure (3).

This Page Intentionally Blank

OCS Facilities Plan Review Process Methodology Flowchart

OCS Facilities Plan Review Process Methodology



Plan Review Guidelines and Implementation Policies

1 Implementation

Maritime security requirements in 33 CFR 106 will be implemented in three distinct phases as outlined below. This "phased-in" methodology allows for rapid deployment of critical regulatory provisions. These phases are:

Implementation Phase (through 31 December 2003) - Key components of this period include:

- CG District Commanders should compile a list of those facilities to which 33 CFR 106 applies. Failure to identify a given facility does not relieve the facility of the obligation to comply with the regulations.
- OCS facilities to which 33 CFR 106 apply should submit an original and one copy along with two electronic copies (on CD) of their Facility Security Plans directly to the National Facility Security Plan Review Center (NFSPRC) in Kansas City that will forward the plans to the Houston Regional Review office for review. Documents should be in Microsoft Word or a compatible format. Drawings should be in AutoCAD or a compatible format. A letter acknowledging receipt of the plan will be forwarded to the submitter.
- The plan will be reviewed in two stages. The Houston Regional Review office will conduct a Stage I plan review, which will be limited to a cursory review to ensure that all required components of the plan are present. The checklist utilized by the reviewers during this process is attached as Enclosure (4) of this NVIC. If minor deficiencies in the FSP are found at this stage, the FSP will continue through the review process before being returned for corrections. However, if major deficiencies are noted during the Stage I review, the FSO will be returned immediately.
- Following the Stage I plan review, a Stage II plan review will be conducted at the regional review office in Houston. This review is much more detailed, assessing the FSP's compliance with every regulatory requirement. This stage also includes an in-depth evaluation of the submitted Facility Security Assessment (FSA) report and the Facility Vulnerability and Security Measures Summary (Form CG-6025). The checklist utilized for Stage II is in Enclosure (5).
- Facilities successfully completing this review stage will receive an approval letter meeting the requirements of 33 CFR 106.115(b).

Pre-Enforcement Phase (1 January 2004 – 30 June 2004) – Key components of this period include:

- Continue Stage I and II plan review for all submitted plans at the Houston office. Plan reviewers will correspond directly with plan submitters.
- Following issuance of an approval letter, two copies of the plan and checklists will be forwarded to the cognizant CG District Commander for commencement of Compliance Verification.
- Compliance Verification will include a more detailed comparison of the FSA with the approved FSP to ensure the adequacy of documented mitigation strategies and that detailed security measures are reasonable and appropriate considering the nature and

location of operations. Following review by the CG District Commander, the approved plan will be forwarded to the cognizant COTP for the Compliance Verification inspection during the next scheduled annual inspection.

- Discrepancies discovered during the Compliance Verification Inspection may result in the requirement that an amendment be submitted to the CG District Commander.
- CG District Commanders will initiate communications with those facilities identified as not having submitted an FSP in accordance with the regulations. While enforcement options will be limited during this period, civil penalty action may be warranted for those facilities not complying with plan submission requirements.

Enforcement Phase (*Commencing* 1 July 2004) – Key components of this period include:

- All regulated facilities should comply with submitted FSP.
- Continue of plan review as necessary.
- Begin Compliance Verification inspection program. This Compliance Verification inspection program consists of an annual compliance inspection following the on-site verification, witnessing at least one exercise every 5 years, and a 5-year plan review activity.

  Note: During the 5-year period, at least one exercise should be coordinated to occur during the annual compliance inspection.
- Initiate active enforcement strategies (enforcement discussed in separate guidance).

2 Initial Submission Process

Understanding the plan review process is critical to the successful implementation of maritime security regulations. The following is a brief discussion on each critical aspect in this process.

2.1 Identification of all Applicable Facilities

In order for CG District Commanders to properly manage this program, they should develop a list identifying all facilities to which 33 CFR 106 applies. They will do this in conjunction with the Minerals Management Service (MMS) and other governmental agencies.

2.2 Submission of Facility Security Plans

In accordance with Reference (a), all facilities to which this part applies should submit Facility Security Plans to the cognizant CG District Commander by 31 December 2003. These plans should be postmarked by the above date. To expedite the initial review, facilities are encouraged to submit their plans directly to:

National Facility Security Plan Review Center
Attn: Security Officer
6601 College Boulevard
Overland Park, KS 66211
1-866-FSP-USCG

After commencement of the enforcement phase (01 July 2004), facilities should submit their plans to the cognizant CG District Commander.

2.3 Communication Strategy

Coast Guard personnel located at the NFSPRC will log the receipt of each FSP and open a Plan Review Activity within the Marine Information for Safety and Law Enforcement system (MISLE). A letter will then be mailed to the plan submitter indicating receipt of the plan and the plan will be forwarded to the Houston Regional Review office for review. This letter will also contain two numbers specific to their facility. The first number will be one of the following depending upon the type of facility:

Table 3-1: Facility Types and Their Numbers

Facility Type	Identification Number
Fixed OCS Facility	Facility Identification Number (FIN)
US Flag MODU, TLP, Spar	Documentation Number
Foreign MODU	IMO Number

The second number will be an Activity Number. These numbers are important to the plan submitter as they will be utilized to remotely check the status of their plan via CG websites, reducing the burden to CG help desk personnel while providing real-time, 24-hour plan review status updates. Once this notification has been received, plan review status will be available via a link available from the USCG Office of Compliance (G-MOC) website at http://www.uscg.mil/hq/g-m/nmc/compl/. Plan submitters will receive written notification when the Central Plan Review Office has received their plan. Visitors to this link must provide the correct Activity Number to access any data. This Activity Number is unique and is not available to anyone outside the Coast Guard. If the desired information not be available through this website, FSP submitters may contact the MTSA HelpDesk at (202) 366-9991 for assistance. Coast Guard personnel will have additional access to this data through the MISLE MARS cube search functions.

3 Administrative Procedures

3.1 Annual Inspection Requirements

Coast Guard personnel will continue to examine/inspect facilities on an annual basis as before. The implementation of 33 CFR 101 - 106 imposes numerous additional security regulations that

should be verified on a regular basis by Coast Guard personnel. Enclosure (6) of this NVIC includes those security items that will be verified by the marine inspector during the annual inspection. As regulations do not require facilities to comply with their FSP until 1 July 2004, Compliance Verification inspections conducted before this date would be voluntary and would not have a compliance aspect to them.

3.2 General Compliance/Enforcement Options

Sanctions for failing to comply with the maritime security regulations are listed in 33 CFR 101.410(c). They include restricting facility access, conditions/suspension of facility operations, lesser administrative measures including civil penalties, or suspending/revoking a FSP. Enforcement compliance actions will be addressed in forthcoming guidance.

3.3 Pre-Enforcement Phase Compliance Options

During the Pre-Enforcement Phase, compliance actions will be directed toward those facilities that do not submit timely FSPs or fail to meet deadlines set in FSP plan review correspondence. Enforcement compliance actions will be addressed in forthcoming guidance.

3.4 Enforcement Phase Compliance Options

During the Enforcement Phase, compliance actions will be directed toward those facilities that are not in compliance with 33 CFR 106. Enforcement and compliance actions may include the suspension of operations for these facilities. Enforcement compliance actions will be addressed in forthcoming guidance.

3.5 MISLE Activity Methodology

Enhancements have been made to the Marine Information for Safety and Law Enforcement (MISLE) database to assist in tracking the progress of FSP through the plan review process and more accurately capture inspection types. For more information on using MISLE applications, you can access several MISLE user guides by visiting MISLENET on the Web: http://mislenet.osc.uscg.mil/user_guides.aspx.

4 Implementation Schedule

Existing facilities are required to submit their FSAs and FSPs by December 31, 2003. The facility is not required to operate in accordance with their plan until July 1, 2004. During this interim period, one or more of the following three letters may be issued by the CG District.

Table 3-2: Letters and Their Purposes

Letter	Purpose
Acknowledgement of Receipt	Advises submitter that NFSPRC has received their plan.
FSP Noncompliance Letter	Informs facility that FSP is in non-compliance or missing. Requires facility to resubmit.
FSP Approval Letter	Final approval letter for FSP issued for a 5-year period.

Upon successful completion of Stage I and II reviews, the NFSPRC will forward the plans and checklists to CG District Commander for issuance of an approval letter. Once the CG District Commander has issued the approval letter, the District will conduct their portion of the Compliance Verification process. Upon completion of the District's review, one copy of the plan will be forwarded to the cognizant COTP for completion of the Compliance Verification inspection. If a substantial problem is discovered during the Compliance Verification process, a letter requiring an amendment will be issued.

5 Alternative Security Programs

Approved alternative security programs (ASPs) are permitted in place of the regulations for OCS facilities found in 33 CFR Part 106. Commandant (G-MP) is the authority to approve these alternatives. As of the writing of this NVIC, there are no approved alternative security programs for the OCS industry. Approved programs will be listed in future revisions to 33 CFR 101.125.

Stage I (Preliminary Review) Guidance

United States Coast Guard

STAGE 1 - USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: _____ OPFAC Number: _____
Facility Name: _____ Facility Type: _____
Reviewer: _____ QA Reviewer: _____ MISLE Activity #:_____

FSP Content Requirements:	***Complete***	***Incomplete***
(1) Security organization of the OCS facility; *Does the plan detail a security organization structure, which includes duties and responsibilities?*	☐	☐
(2) Personnel training; *Are personnel training requirements relative to the appropriative FSP provisions addressed?*	☐	☐
(3) Drills and exercises; *Does the plan detail drill & exercise requirements that validate plan processes and test the proficiency of facility personnel in assigned security duties at all MARSEC levels?*	☐	☐
(4) Records and documentation; *Facility recordkeeping procedures are identified that ensure all relevant information is available to document plan review and approval, training, security incidents and breaches, changes in MARSEC levels, etc...*	☐	☐
(5) Response to change in MARSEC Level; *Procedures are identified for MARSEC level coordination & implementation of security requirements.*	☐	☐
(6) Procedures for interfacing with vessels; *Does the FSP address procedures for interfacing with vessels at all MARSEC levels?*	☐	☐
(7) Declaration of Security (DOS); *The FSP identifies procedures for using DOS's.*	☐	☐
(8) Communications; *Procedures for notifying facility personnel of changes in security conditions have been identified.*	☐	☐
(9) Security systems and equipment maintenance; *Procedures for inspection, testing, calibration, and maintenance of security equipment are addressed.*	☐	☐
(10) Security measures for access control; *Procedures for controlling access to the facility, deter unauthorized introduction of unauthorized material/items (dangerous substances & devices, etc) are addressed.*	☐	☐
(11) Security measures for restricted areas; *Does the plan include a restricted area access control process? This includes procedures to deter unauthorized access, protect persons authorized to be in the facility, protect cargo & vessel stores from tampering etc.*	☐	☐
(12) Security measures for delivery of stores and industrial supplies; *Does the plan address the security requirements relating to the delivery of stores & industrial supplies at all MARSEC levels?*	☐	☐
(13) Security measures for monitoring; *Does the FSP identify security measures to ensure continuous monitoring of the facility? This may include the capability to continuously monitor, through lighting, patrols, and surveillance equipment.*	☐	☐
(14) Security incident procedures; *The FSP contains procedures for addressing security incidents including the following: response to security threats; evacuation of the facility; report security incidents.*	☐	☐
(15) Audits and FSP amendments; *The FSP identifies procedures for auditing & updating the plan.*	☐	☐

United States Coast Guard

STAGE 1 – USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: ____________________________ OPFAC Number: ________________________________
Facility Name: ____ Facility Type: ___________________________________

Item:	*Incomplete Reason:*

Note: *If two or more of content requirements 1-15 are incomplete, then the FSP is to be returned to originator for correction before going to stage 2 review*

This Page Intentionally Blank

Stage II (Detailed FSP Review) Guidance

United States Coast Guard

STAGE 2 - USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
General;				
106.400 General				
1. All portions of the submitted FSP shall be written in English?	☐	☐	☐	☐
2. Are procedures identified for protecting and handling the FSP as "Sensitive Security Information" in accordance with 49 CFR Part 1520?	☐	☐	☐	☐
106.410 Submission and approval				
1. Has a letter been included that certifies that the FSP meets all applicable requirements of 33 CFR Part 106?	☐	☐	☐	☐
106.410 Submission and approval				
1. If two or more OCS Facilities are included in the same FSP, the facilities should share similarities in physical characteristics, location, and operations?	☐	☐	☐	☐
(1) Security organization of the OCS facility;				
106.200 Owner or operator				
1. Has the security organizational structure for the OCS facility been defined?	☐	☐	☐	☐
2. Does the FSP designate a Company Security Officer (CSO) by either name or title, and describe the duties and responsibilities of this officer?	☐	☐	☐	☐
3. Does the FSP designate a Facility Security Officer (FSO) by either name or title, and describe the duties and responsibilities of this officer? *[Note: the CSO and FSO may be the same person, but must be explicitly stated in the FSP]*.	☐	☐	☐	☐
106.210 OCS Facility Security Officer (FSO)				
1. If the FSO serves the duties and responsibilities of an FSO for more than one OCS Facility, is the name for each OCS facility for which he or she is the FSO listed in the FSP of each OCS facility for which he or she is the FSO?	☐	☐	☐	☐
2. If the FSO serves the duties and responsibilities of an FSO for more than one OCS Facility, are the OCS facilities in reasonable proximity to each other?	☐	☐	☐	☐
106.400 General				
1. Does the FSP provide 24 hour contact information for the FSO?	☐	☐	☐	☐
106.200 Owner or operator				
1. Does the FSP establish measures to ensure that the OCS facility can implement additional security measures required for an increase in **MARSEC Level** within a 12 hour period?	☐	☐	☐	☐
2. Does the FSP establish procedures to notify the National Response Center to report suspicious activities that may result in a Transportation Security Incident (TSI)?	☐	☐	☐	☐
3. Does the FSP establish procedures to notify the cognizant District Commander	☐	☐	☐	☐

United States Coast Guard

STAGE 2 - USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	***Satisfactory***	***Not Satisfactory***	***Pending 3rd Stage***	***Not Applicable***
immediately following a breach in security or Transportation Security Incident (TSI)?				
(2) Personnel training; **106.220 Security training for all other OCS facility personnel** 1. Does the FSP include provisions to provide training to OCS Facility personnel, including both full-time and part-time contractors, temporary and permanent employees?	☐	☐	☐	☐
2. Do the training standards for those persons requiring training include the following?				
2.1. Relevant provisions of the FSP;	☐	☐	☐	☐
2.2. The meaning and the consequential requirements of the different **MARSEC Levels** including emergency procedures and contingency plans;	☐	☐	☐	☐
2.3. Recognition and detection of dangerous substances and devices;	☐	☐	☐	☐
2.4. Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; and	☐	☐	☐	☐
2.5. Recognition of techniques used to circumvent security measures.	☐	☐	☐	☐
(3) Drills and exercises; **106.225 Drill and exercise requirements** 1. Does the FSP include provisions to ensure the OCS Facility conducts a minimum of one drill every 3 months?	☐	☐	☐	☐
2. Does the FSP include provisions to ensure the OCS Facility conducts an exercise at least once every calendar year, with not more than 18 months between exercises?	☐	☐	☐	☐
3. Does the FSP include provisions to ensure that exercises test communication and notification procedures, and elements of coordination, resource availability, and response?	☐	☐	☐	☐
(4) Records and documentation; **106.230 OCS facility record keeping requirements** 1. Does the FSP include provisions to maintain the following records, either in paper or electronic format?				
1.1. Training;				
1.1.1. For each security training session, do the training records include the date of each session, duration of each session, a description of the training, and a list of attendees?	☐	☐	☐	☐
1.2. Drills and Exercises;				
1.2.1. For each drill or exercise, do the drill/exercise records include the date it was held, a description of the drill/exercise, a list of participants, and any best practices learned which may improve	☐	☐	☐	☐

United States Coast Guard

STAGE 2 - USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	***Satisfactory***	***Not Satisfactory***	***Pending 3rd Stage***	***Not Applicable***
the FSP? 1.3. Incidents and breeches of security; 1.3.1. For each breach of security or security incident, do the records include the date & time of the occurrence, locations within the OCS facility the security breach occurred, a description of the breach, the identity of the individual to whom it was reported, and a description of the response?	☐	☐	☐	☐
1.4. Changes in **MARSEC Levels**; 1.4.1. For each change in **MARSEC Level**, do the records include the date and time of the notification was received and the time the OCS facility was in compliance with the additional requirements?	☐	☐	☐	☐
1.5. Maintenance, calibration, and testing of security equipment; 1.5.1. For each occurrence of maintenance, calibration, and testing, do the maintenance records include the date & time, and the specific security equipment involved?	☐	☐	☐	☐
1.6. Security threats; 1.6.1. For each security threat, do the records include the date & time of the occurrence, how the threat was communicated, who received or identified the threat, a description of the threat, to whom it was reported, and a description of the response?	☐	☐	☐	☐
1.7. Declaration of Security (DOS); 1.7.1. Are copies of each DOS maintained for at least 90 days following the effective period of that DOS?	☐	☐	☐	☐
1.8. Annual audit of the Facility Security Plan; 1.8.1. For each annual audit, do the records include letters certified by the FSO stating that the audit was conducted?	☐	☐	☐	☐
2. Does the FSP stipulate that records must be maintained for each section (with the exception of DOS's) for a minimum of 2 years?	☐	☐	☐	☐
(5) Response to change in MARSEC Level; **106.235 Maritime Security (MARSEC) Level coordination and implementation** 1. Does the FSP describe how vessels interfacing with the OCS facility within 96 hours of an increase in **MARSEC Level** will be notified of that **MARSEC Level** change?	☐	☐	☐	☐
2. Does the FSP include provisions describing how the cognizant District Commander will be contacted to report compliance or non-compliance of an increase in **MARSEC Level**?	☐	☐	☐	☐
(6) Procedures for interfacing with vessels; **106.245 Procedures for interfacing with vessels** 1. Does the FSP contain provisions for interfacing with vessels for : 1.1. **MARSEC Level 1**; 1.2. **MARSEC Level 2**; and	☐ ☐	☐ ☐	☐ ☐	☐ ☐

United States Coast Guard

STAGE 2 - USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	***Satisfactory***	***Not Satisfactory***	***Pending 3rd Stage***	***Not Applicable***
1.3. **MARSEC Level 3**?	☐	☐	☐	☐
(7) Declaration of Security (DOS);				
105.250 Declaration of Security (DOS)				
1. Does the FSP establish procedures for requesting a DOS and handling DOS requests from vessels that interface with the OCS facility?	☐	☐	☐	☐
2. If the FSP contains provisions for continuing DOS's, does it stipulate the expiration requirements? *(**MARSEC Level 1** = 90 days, **MARSEC Level 2** = 30 days)*	☐	☐	☐	☐
(8) Communications;				
106.240 Communications				
1. Does the FSP describe how the FSO will notify personnel of changes in security conditions at the OCS facility?	☐	☐	☐	☐
2. Does the OCS Facility have a backup means for both internal and external communications?	☐	☐	☐	☐
(9) Security systems and equipment maintenance;				
106.255 Security systems and equipment maintenance				
1. Does the FSP include procedures for identifying and responding to security system and equipment failures or malfunctions?	☐	☐	☐	☐
(10) Security measures for access control;				
106.260 Security measures for access control				
1. Does the submitted FSP describe how the access control security measures will;				
1.1. Deter the introduction of unauthorized substances & devices;	☐	☐	☐	☐
1.2. Secure dangerous substances & devices that are authorized to be on board;	☐	☐	☐	☐
1.3. Control access to the OCS facility?	☐	☐	☐	☐
2. Are the following security measures addressed for **MARSEC Level 1**;				
2.1. Screening of persons and personnel effects going on board;	☐	☐	☐	☐
2.2. Posting of signs stating the security measures in effect;	☐	☐	☐	☐
2.3. Checking of identification of persons seeking to board;	☐	☐	☐	☐
2.4. Deterrence of unauthorized access;	☐	☐	☐	☐
2.5. Access points that must be secured or attended are identified;	☐	☐	☐	☐
2.6. Access to unattended spaces that adjoin areas which passengers and visitors have access are locked or otherwise prevented;	☐	☐	☐	☐
2.7. Personnel are not required to be subjected to screening by other personnel, unless security clearly requires it;	☐	☐	☐	☐
2.8. A designated secure area for conducting inspections and screening is	☐	☐	☐	☐

United States Coast Guard

STAGE 2 - USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	***Satisfactory***	***Not Satisfactory***	***Pending 3rd Stage***	***Not Applicable***
designated; and 2.9. Responding to the presence of unauthorized persons on board?	☐	☐	☐	☐
3. Does the submitted FSP describe in detail the additional or increased security measures for access control at the OCS Facility for; 3.1. **MARSEC Level 2**; 3.2. **MARSEC Level 3**?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
(11) Security measures for restricted areas; **106.265 Security measures for restricted areas** 1. Does the submitted FSP describe how the restricted area security measures will; 1.1. Prevent and deter unauthorized access; 1.2. Protect persons authorized to be on board; 1.3. Protect the OCS facility; 1.4. Protect vessels interfacing with the OCS facility; 1.5. Protect sensitive security areas within the OCS facility; 1.6. Protect security & surveillance equipment / systems; and 1.7. Protect stores & industrial supplies from tampering?				
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
2. Does the FSP include measures for restricted areas to; 2.1. Identify which personnel are authorized to have access; 2.2. Determine which persons other than OCS facility personnel are authorized access; 2.3. Determine under which conditions access may take place; 2.4. Define the extent of a restricted area; and 2.5. Define the times when access restrictions apply?				
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
3. Are security measures in place to ensure the prevention unauthorized access to activities within restricted areas at **MARSEC Level 1**?	☐	☐	☐	☐
4. Does the submitted FSP describe in detail the additional or increased security measures for restricted areas at the OCS Facility for; 4.1. **MARSEC Level 2**; and 4.2. **MARSEC Level 3**?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
(12) Security measures for delivery of stores and industrial supplies; **105.270 Security measures for delivery of stores and industrial supplies** 1. Does the submitted FSP describe how the security measures for the delivery of stores & industrial supplies will; 1.1. Check stores & industrial supplies for package integrity; 1.2. Prevent stores & industrial supplies from being accepted without inspection; 1.3. Deter tampering; 1.4. Prevent stores & industrial supplies from being accepted unless ordered;				
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐
	☐	☐	☐	☐

United States Coast Guard

STAGE 2 - USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	***Satisfactory***	***Not Satisfactory***	***Pending 3rd Stage***	***Not Applicable***
and 1.5. Protect security & surveillance equipment / systems?	☐	☐	☐	☐
2. Are the following security measures for accepting stores & industrial supplies addressed for **MARSEC Level 1**; 2.1. Inspecting stores & industrial supplies before being accepted; and 2.2. Checking that stores or industrial supplies match the order being brought on board?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
3. Does the submitted FSP describe in detail the additional or increased security measures for the delivery of stores & industrial supplies at the OCS Facility for; 3.1. **MARSEC Level 2**; and 3.2. **MARSEC Level 3**?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
(13) Security measures for monitoring; **106.275 Security measures for monitoring** 1. Does the submitted FSP describe how the OCS facility will have the capability to monitor restricted areas on board the OCS facility and the area surrounding the facility?	☐	☐	☐	☐
2. Are the following monitoring security measures addressed for **MARSEC Level 1**; 2.1. Monitoring the OCS facility, including restricted areas and access points?; 2.2. The ability to conduct emergency searches; 2.3. Ensuring that equipment or system failures are identified & corrected; 2.4. Ensuring automatic intrusion systems have alarms, and are continually attended or monitored; and 2.5. Ensuring the deck is lighted during periods between sunset & sunrise and periods of limited visibility?	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐
3. Does the submitted FSP describe in detail the additional or increased security measures for the delivery of stores & industrial supplies at the OCS Facility for; 3.1. **MARSEC Level 2**; and 3.2. **MARSEC Level 3**?	☐ ☐	☐ ☐	☐ ☐	☐ ☐
(14) Security incident procedures; **106.280 Security incident procedures** 1. Does the submitted FSP describe how the FSO and OCS facility security personnel are able to: 1.1. Respond to security threats or breaches of security and maintain critical OCS facility and OCS facility-to-vessel interface operations? 1.2. Deny access to the OCS facility, except those responding to an emergency?	☐ ☐	☐ ☐	☐ ☐	☐ ☐

United States Coast Guard

STAGE 2 - USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	***Satisfactory***	***Not Satisfactory***	***Pending 3rd Stage***	***Not Applicable***
1.3. Evacuate the OCS facility in case of security threats or breaches of security?	☐	☐	☐	☐
1.4. Report security incidents to the National Response Center and the cognizant District Commander?	☐	☐	☐	☐
1.5. Brief all OCS facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities?	☐	☐	☐	☐
1.6. Secure non-critical operations in order to focus response on critical operations?	☐	☐	☐	☐
(15) Audits and FSP amendments;				
106.415 Amendment and audit				
1. Does the FSP contain procedures to conduct audits annually?	☐	☐	☐	☐
2. Does the FSP contain procedures to initiate, develop & submit amendments?	☐	☐	☐	☐
(16) Facility Security Assessment (FSA) report;				
106.305 Facility Security Assessment (FSA) requirements				
1. Does the FSA report include the following items;				
1.1. A summary of how the on-scene survey was conducted;	☐	☐	☐	☐
1.2. A description of each vulnerability found during the on-scene survey;	☐	☐	☐	☐
1.3. A description of existing security measures, including the following;	☐	☐	☐	☐
1.4. Inspection;	☐	☐	☐	☐
1.5. Control and monitoring equipment;	☐	☐	☐	☐
1.6. Personnel identification documents;	☐	☐	☐	☐
1.7. Communication;	☐	☐	☐	☐
1.8. Lighting;	☐	☐	☐	☐
1.9. Alarm systems;	☐	☐	☐	☐
1.10. Access Control;	☐	☐	☐	☐
1.11. A list of the key OCS facility operations that are important to protect; and	☐	☐	☐	☐
1.12. A list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the OCS Facility?	☐	☐	☐	☐
2. Does the FSA report describe the following elements within the OCS facility;				
2.1. Physical security;	☐	☐	☐	☐
2.2. Structural integrity;	☐	☐	☐	☐
2.3. Personnel protection systems;	☐	☐	☐	☐
2.4. Procedural policies; and	☐	☐	☐	☐
2.5. Radio / telecommunication systems, including computer systems & networks; and	☐	☐	☐	☐
2.6. Essential services?	☐	☐	☐	☐

United States Coast Guard

STAGE 2 - USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	***Satisfactory***	***Not Satisfactory***	***Pending 3rd Stage***	***Not Applicable***

United States Coast Guard

STAGE 2 - USCG OCS FACILITY SECURITY PLANS (FSP) REVIEW FORM

Facility Identification Number: ____________________________ OPFAC: ____

Facility Name: ____ Facility Type: ___________________________________

Item:	***Incomplete Reason:***

Compliance Verification Procedures

The Compliance Verification field guide will be distributed at a later date under separate correspondence.

Sample Correspondence

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

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-MOC
Phone: (202) 267-0495
Fax: (202) 267-0506

SSIC
Date
MISLE Activity # XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE PLAN RECEIPT LETTER

Dear Mr./Ms. XXXX:

We are in receipt of your Facility Security Plan dated *[Date]*, for the [*Facility Name]*.

You may periodically check the status of the review of your security plan by accessing the Coast Guard Marine Information Exchange website at www.cgxxxxx. To obtain status information, you will need to enter your MISLE Activity number listed above as your log-on ID.

We thank you for your submission and remind you to move forward in the development of your security program. Should you have any further questions with reference to your plan review, please contact Lieutenant K.C. Office at (866) 377-8724.

Sincerely,

K. C. OFFICE
Lieutenant, U.S. Coast Guard
National Facility Security Plan Review Center
By direction

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

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-MOC
Phone: (202) 267-0495
Fax: (202) 267-0506

SSIC
Date
MISLE Activity # XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE STAGE I FAILURE LETTER

Dear Mr./Ms. XXXX:

We have completed a Stage I review of your submitted facility security plan dated *[date]* for *[Company Name]*. Regrettably, your plan does not meet the requirements as outlined in 33 CFR Part 106 and is being returned for correction. Below is a summary of the essential element(s) missing in your plan. These element(s) should be addressed adequately and the plan returned to this office no later than 30 days from the date of this letter. Once these items have been addressed to our satisfaction, we will forward your plan for further review.

1) Your plan has omitted any discussion on **Drills and Exercises**.

2) Procedures for **Interfacing with vessels** have been omitted.

Should you have any further questions concerning your facility security plan review, please contact Lieutenant K.C. Office at (866) 377-8724.

Sincerely,

K. C. OFFICE
Lieutenant, U.S. Coast Guard
National Facility Security Plan Review Center
By direction

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

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-MOC
Phone: (202) 267-0495
Fax: (202) 267-0506

SSIC
Date
MISLE Activity # XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE STAGE II PROBLEM LETTER

Dear Mr./Ms. XXXX:

We have completed a Stage II review of your submitted facility security plan dated *[date]* for *[Company Name]*. Unfortunately, your plan does not meet the requirements as outlined in 33 CFR Part 106. Below is a summary of the element(s) missing in your plan. These deficiencies should be corrected and re-submitted to this office no later than 30 days from the date of this letter. Once these items have been addressed to our satisfaction, we will forward your plan for further review.

1) Your plan has not addressed which **access control** measures will be in place along the northern perimeter your facility.

Should you have any further questions concerning your facility security plan review, please contact Lieutenant K.C. Office at (866) 377-8724.

Sincerely,

K. C. OFFICE
Lieutenant, U.S. Coast Guard
National Facility Security Plan Review Center
By direction

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

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-MOC
Phone: (202) 267-0495
Fax: (202) 267-0506

SSIC
Date
MISLE Activity # XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE LETTER OF AUTHORIZATION TO OPERATE LETTER

Dear Mr./Ms. XXXX:

The facility security plan (FSP) for [*Facility Name]*, submitted to meet the requirements of Title 33 Code of Federal Regulations (CFR) Part 106, is currently under review by the U.S. Coast Guard. *[Facility Name]* may continue to operate in accordance with all the provisions of the submitted plan pending final determination of FSP approval. This Letter of Authorization will expire on *[date / up to one year]*, at which time the Coast Guard will reevaluate the status and progress of your plan submission.

Commencing July 1, 2004, [*Facility Name]* should operate in full compliance with their submitted FSP and any additional requirements contained in 33 CFR Part 106. You are reminded that any deviation from this submitted plan requires immediate notification to this office. Your facility security plan is sensitive security information and should be protected in accordance with 49 CFR Part 1520. A copy of your security plan and any amendments should be made available to Coast Guard personnel upon request.

We will continue to work closely with you in developing a security plan that reflects your company's operating procedures and organizational structure. Please ensure that all parties with responsibilities under these plans are familiar with the procedures and requirements contained therein. If you have any questions, please contact *XXXX* at *(XXX) XXX-XXXX*.

Sincerely,

Captain of the Port or
Designated representative

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

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-MOC
Phone: (202) 267-0495
Fax: (202) 267-0506

SSIC
Date
MISLE Activity # XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE PLAN APPROVAL LETTER

Dear Mr./Ms. XXXX:

The facility security plan for [*Facility Name]*, submitted to meet the requirements of Title 33 Code of Federal Regulations (CFR) Part 106, is approved.

Commencing July 1, 2004, [*Company/Facility Name]* should operate in compliance with this approved security plan and any additional requirements contained in 33 CFR Part 106. You are reminded that you should report to this office any deviation from this approved plan immediately. Your facility security plan is sensitive security information and should be protected in accordance with 49 CFR Part 1520. A copy of your security plan and any amendments should be made available to Coast Guard personnel upon request.

This approval will remain valid until five years from the date of this letter unless rescinded in writing by this office. You should review your plans annually and submit any amendments to this office for re-approval as required by Title 33, CFR Part 106.410 and 106.415. **Keep a copy of this letter with the security plan.** Coast Guard personnel will audit your adherence with the requirements of this plan on an annual basis

I commend your efforts in developing a security plan that reflects your company's operating procedures and organizational structure. Implementation of the strategies and procedures contained in your plan serve to reduce the risk and mitigate the results of an act that threatens the security of personnel, the facility, and the public. Please ensure that all parties with responsibilities under these plans are familiar with the procedures and requirements contained therein. If you have any questions, please contact *XXXX* at *(XXX) XXX-XXXX*.

Sincerely,

Captain of the Port or
Designated representative

GUIDANCE FOR SUBMISSION OF ALTERNATIVE SECURITY PROGRAM (ASP)

GUIDANCE FOR SUBMISSION OF ALTERNATIVE SECURITY PROGRAM (ASP)

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, 105, or 106 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 or implementing a security plan tailored to their specific vessel or facility.

APPLICATION REQUIREMENT

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.

An ASP that only addresses intended alternatives is not sufficient.

PROGRAM SUBMISSION

ASPs 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

Each package must contain a

- Point of contact,
- Mailing address, and
- Telephone number.

ACTION UPON RECEIPT

- Applications will be reviewed on a first-come, first-served basis.

- 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.

- 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.

- 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 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. The organization will then have to make corrections and resubmit the program.

COMPLIANCE

On or before December 31, 2003 members using a ASP must do the following:

Vessel Owner or Operators 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

Facility Owner or Operators using an ASP must send a letter to the Coast Guard National Plan Review Center or Captain of the Port (COTP) stating which approved ASP they are intending to use to:

Coast Guard National Facility Security Plan Review Center
Mailstop Q6

6601 College Boulevard
Overland Park, Kansas 66211
1-866-FSP-USCG or 1-866-377-8724

- On or before July 1, 2004 members must have the following documentation available to the appropriate COTP for inspection and verification of compliance.

  Vessel Owner or Operators: 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 the vessel is in full compliance with the program.

  Facility Owner or Operators: must have a copy of the ASP the facility is using, including a facility security assessment report and a letter signed by the facility owner or operator stating which ASP the facility is using and certifying that the facility is in full compliance with the program.

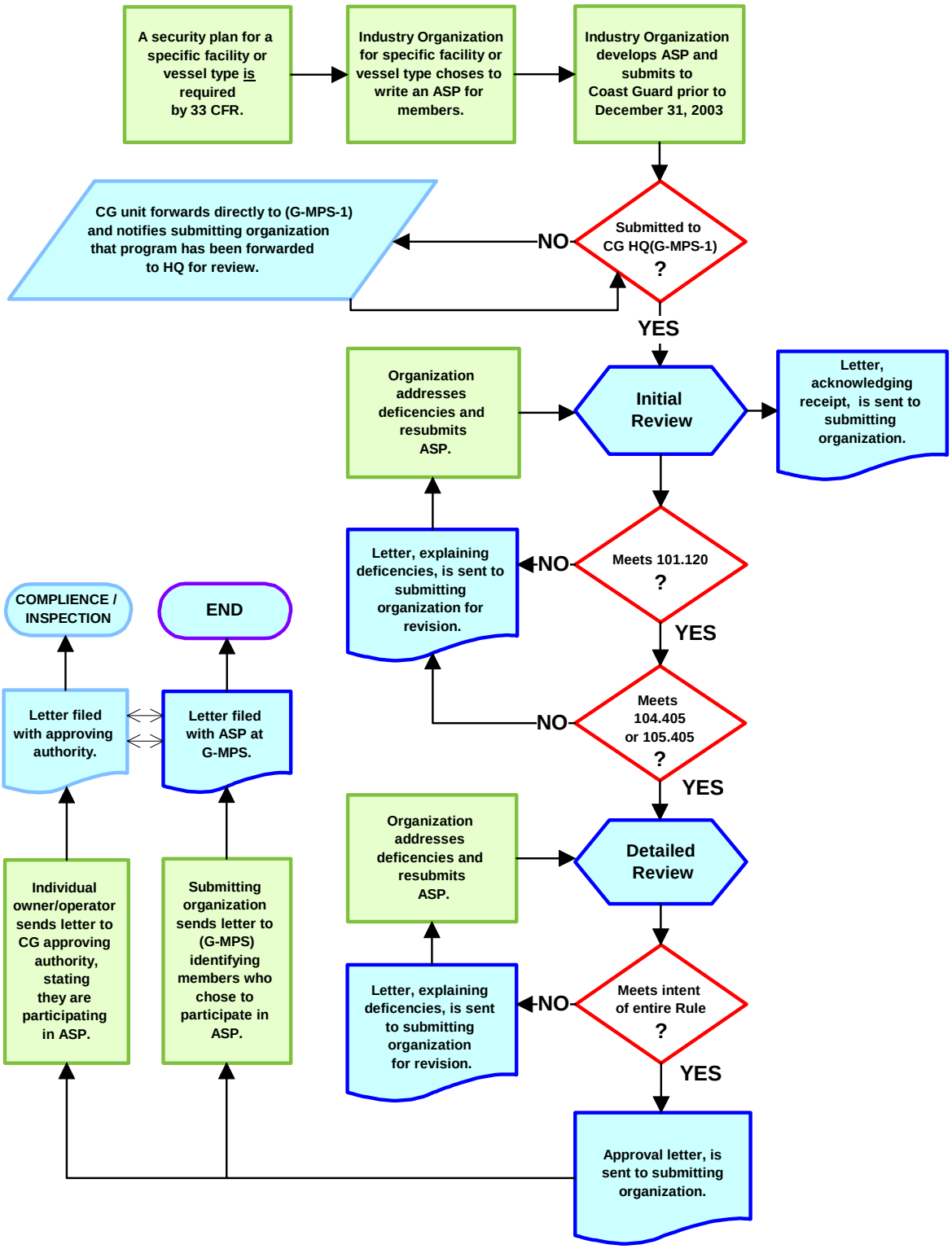
OPERATIONAL SECURITY

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.

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.

ALTERNATIVE SECURITY PROGRAM APPROVAL PROCESS



GUIDANCE FOR SUBMISSION OF EQUIVALENCY REQUESTS OR WAIVER REQUESTS

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 owners or operators to request approval for the use of Equivalent Security Measures (Equivalency Requests) or Waivers of Security Requirements (Waiver Requests).

APPLICATION REQUIREMENTS

EQUIVALENT REQUESTS

For any security measure required by 33 CFR 104, 105, or 106, 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 equivalent request. Each application must contain:

1. The request to use an equivalent security measure.
2. The documentation supporting justification for the request.

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.

REQUEST SUBMISSION

Equivalent requests or Waiver requests and any accompanying documents must be submitted via hard copy paper document, floppy disc, or compact disc (CD). VSPs, FSPs, and ASPs are deemed to contain 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

Each package must contain a

- Point of contact,
- Mailing address, and
- Telephone number.

ACTION UPON RECEIPT

- 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.

- Applications will be reviewed on a first-come, first-served basis.

- 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.

- Applications that pass the initial review will then undergo a detailed review. Coast Guard Headquarters (G-MPS) may request further review and input from Area. Atlantic Area and Pacific Area may disseminate for review as appropriate. All comments must be submitted to G-MPS within one week of Area receiving the request for input. During the detailed review, request content will be examined to determine compliance with the performance standards and at all MARSEC levels.

- 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.

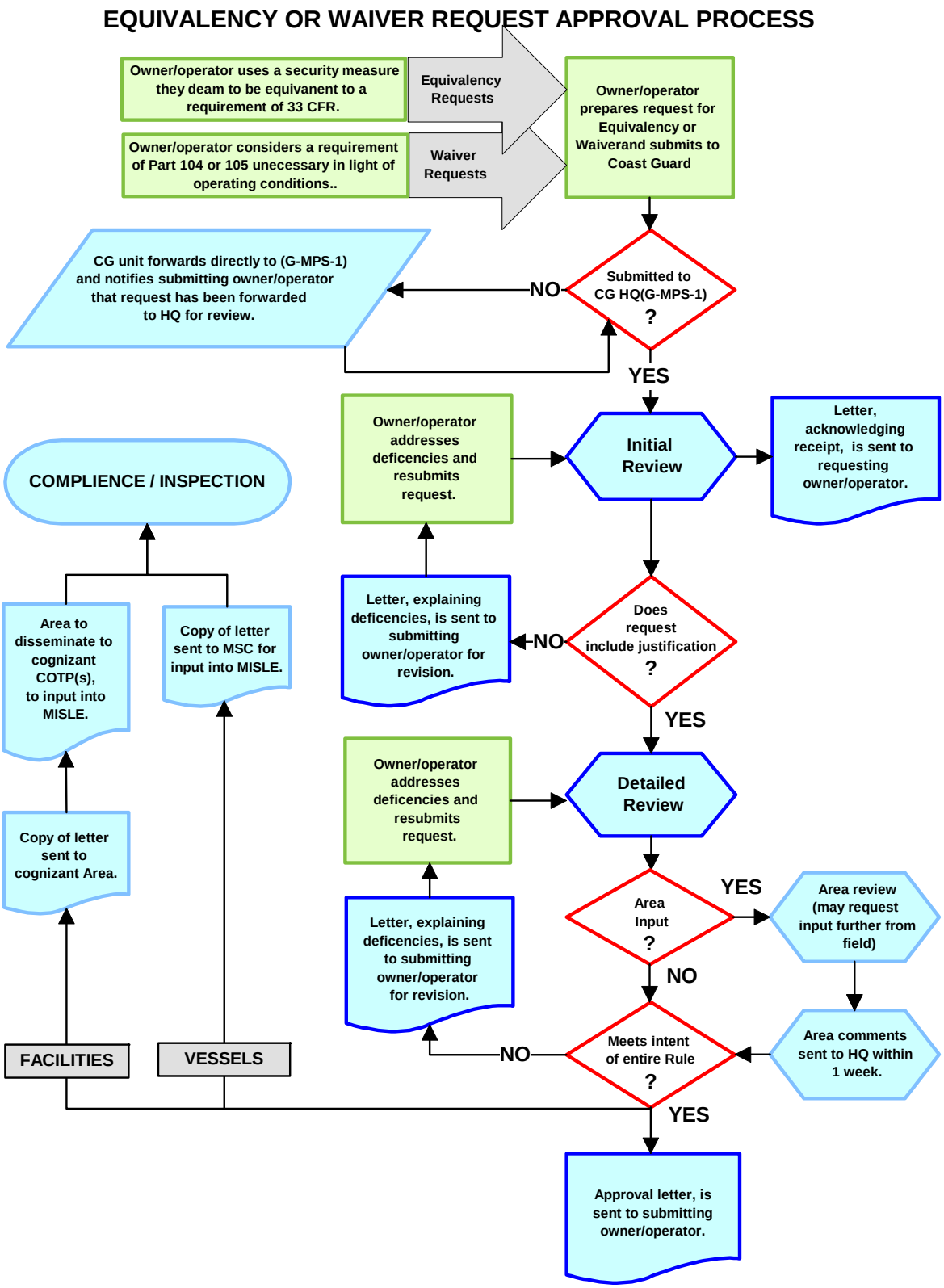
- If the application is disapproved after the detailed review, a copy of the application will be returned to the submitter with a brief statement of the reasons for disapproval. The original application will be kept on file at Coast Guard Headquarters (G-MPS) for future reference.

OPERATIONAL SECURITY

Security plans, including VSPs and FSPs, are considered SSI, and therefore, they are exempt from the Freedom of Information Act (FOIA), meaning that requests for plans and applications under FOIA 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.

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) with 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.


EQUIVALENCY OR WAIVER REQUEST APPROVAL PROCESS
Owner/operator uses a security measure they deam to be equivanent to a requirement of 33 CFR.
Equivalency Requests
Owner/operator considers a requirement of Part 104 or 105 unecessary in light of operating conditions..
Waiver Requests
Owner/operator prepares request for Equivalency or Waiverand submits to Coast Guard
Submitted to CG HQ(G-MPS-1) ?
NO
CG unit forwards directly to (G-MPS-1) and notifies submitting owner/operator that request has been forwarded to HQ for review.
YES
Initial Review
Letter, acknowledging receipt, is sent to requesting owner/operator.
Owner/operator addresses deficencies and resubmits request.
Does request include justification ?
NO
Letter, explaining deficencies, is sent to submitting owner/operator for revision.
YES
Detailed Review
Owner/operator addresses deficencies and resubmits request.
Area Input ?
YES
Area review (may request input further from field)
NO
Letter, explaining deficencies, is sent to submitting owner/operator for revision.
Meets intent of entire Rule ?
NO
Area comments sent to HQ within 1 week.
YES
Approval letter, is sent to submitting owner/operator.
COMPLIENCE / INSPECTION
Area to disseminate to cognizant COTP(s), to input into MISLE.
Copy of letter sent to MSC for input into MISLE.
Copy of letter sent to cognizant Area.
FACILITIES
VESSELS