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) 267-0493
Fax: (202) 267-4394
Email: fldr-g-moc@comdt.uscg.mil

COMDTPUB P16700.4
NVIC 03-03 Change 1
MAY 27 2004

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 03-03, CH-1

Subj: CH-1 TO NVIC 03-03, IMPLEMENTATION GUIDANCE FOR THE REGULATIONS MANDATED BY THE MARITIME TRANSPORTATION SECURITY ACT OF 2002 (MTSA) FOR FACILITIES

1. PURPOSE. The purpose of this circular is to provide further guidance for the implementation of the maritime security regulations mandated by the Maritime Transportation Security Act of 2002 (MTSA). The information contained herein details the plan review process, provides guidance to successfully execute compliance inspections, and provides clarification on the applicability of MTSA mandated regulations found in 33 CFR Part 105.

2. ACTION.

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

   b. Facility owners and operators are encouraged to use this circular as guidance in preparation for MTSA compliance inspections of their facilities by Coast Guard personnel. COTPs shall use this guidance during all MTSA compliance inspections.

3. DIRECTIVES AFFECTED. NVIC 03-03 is revised to provide additional guidance on the Final Rules on Maritime Security, 33 CFR Subchapter H, and the Maritime Transportation Security Act (MTSA) of 2002. Enclosures (10) and (11) are added. Enclosure (7) is modified as the Letter of Authorization (page 5) has been revised and the Interim Letter of Approval (page 7) has been added. The remainder of NVIC 03-03 is unchanged.

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																										

4. BACKGROUND. NVIC 03-03 was published to assist Captain of the Port (COTP) personnel as well as owners and operators of affected facilities in complying with the maritime security regulations. Beginning 1 July 2004, affected facilities must comply with an approved Facility Security Plan (FSP) or Alternative Security Program (ASP).

5. DISCUSSION.

   a. Captain of the Port (COTP) personnel will conduct examinations of affected facilities to determine compliance with 33 CFR 105 and their approved ASP/FSP. Enclosure (10), MTSA Facility Compliance Guide, provides detailed guidance for facility inspectors conducting MTSA compliance examinations and outlines specific performance based criteria based on the regulations found in 33 CFR 105. Completed examination checklists contained in the MTSA Facility Compliance Guide shall be treated as Sensitive Security Information (SSI). It is intended for both COTPs and facility owners and operators to help ensure consistency during facility examinations.

   b. Enclosure (11), Additional Policy Guidance, incorporates recent policy guidance and is intended as a supplement to the existing guidance in NVIC 03-03, the preambles to the Interim Rule and the Final Rule, and other policy guidance promulgated by the Coast Guard. In addition, key Policy Advisory Council (PAC) decisions applicable to MTSA facilities are included. Addendum (1) contains a decision flowchart for issuing Letters of Approval, Interim Letters of Approval, and Letters of Authorization. Addendum (2) contains a Declaration of Security (DoS) applicability decision tool as an aid in determining the requirements for completing a DoS for a wide range of vessel/facility or vessel/vessel interfaces at all MARSEC Levels. Addendum (3) contains a compliance matrix that provides guidance for initiating penalties and operational controls and is intended as a tool to be used by the COTP/OCMI to evaluate a facility's compliance with the regulations found in 33 CFR 105.

   c. As additional guidance continues to be developed, the MTSA-ISPS Helpdesk website http://www.uscg.mil/hq/g-m/mp/MTSA.shtml should be consulted regularly for the most up to date policy guidance and information.

   d. MTSA regulations do not mandate specific equipment or procedures, but call for performance based criteria to ensure the security of the facility. The MTSA Facility Compliance Guide is designed to assess not only the facilities compliance with their approved FSP or ASP, but the adequacy of the FSP/ASP with performance criteria outlined in the regulations.

6. IMPLEMENTATION.

   a. The implementation of the maritime security regulations for facilities mandated by the Maritime Transportation Security Act of 2002 will be executed in two distinct phases:

      (1) FSP Review & Approval Phase (1 January 2004 through 30 June 2004)

(2) Compliance Phase (1 July 2004 and beyond)

b. COTPs shall issue, as appropriate for those facilities that have submitted an FSP for review, a Letter of Approval, an Interim Letter of Approval, or a Letter of Authorization in accordance with the guidance and timelines specified in enclosure (11).

c. COTPs shall use the MTSA Facility Compliance Guide, enclosure (10), while conducting facility compliance examinations beginning July 1, 2004. COTPs shall actively distribute this guide to all MTSA facilities within their fleet of responsibility by all appropriate means and encourage its use to enhance compliance.

7. INFORMATION SECURITY.

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

b. Under these regulations, only persons with a "need to know," as defined in 49 CFR 1520.11, will have access to security assessments, plans and amendments. Vessel and facility owners or operators must determine which of their employees need to know which provisions of the security plans and assessments and restrict dissemination of these documents accordingly. To ensure that access is restricted to only authorized personnel, SSI material will not to be disclosed under the Freedom of Information Act (FOIA) under almost all circumstances.

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

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

9. CHANGES. This NVIC will be posted on the web at www.uscg.mil/hq/g-m/nvic/index00.htm. Changes to this circular will be issued as necessary. Time-sensitive

amendments will be issued as "urgent change" messages by ALDIST/ALCOAST and posted on the website for the benefit of industry, pending their inclusion to the next change to this circular. Suggestions for improvements of this circular should be submitted in writing to Commandant (G-MOC).

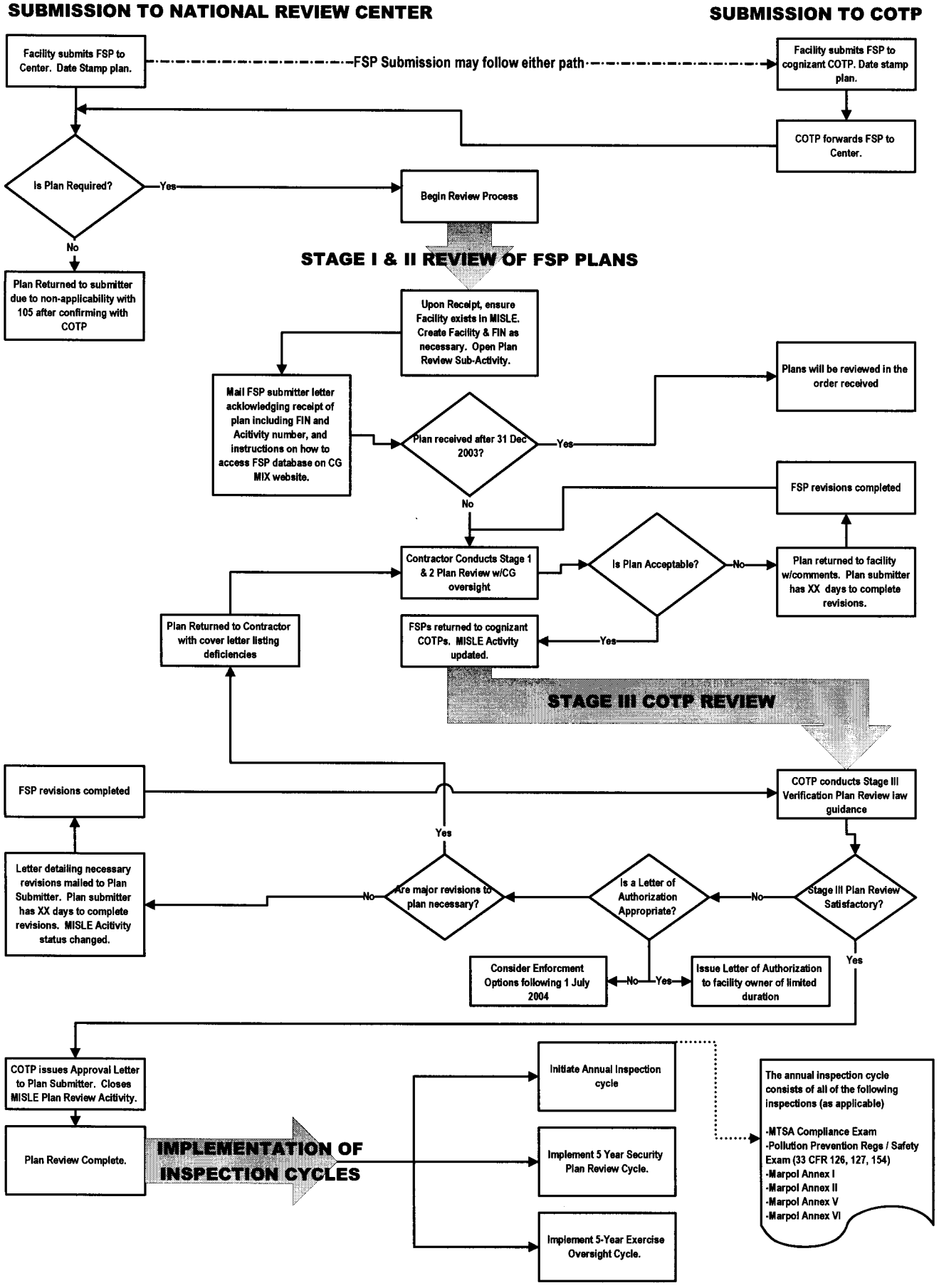
THOMAS H. GILMOUR
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Marine Safety, Security
And Environmental Protection

Encl (7) Letter of Authorization (pg. 5) and Interim Letter of Approval (pg.7), CH-1
Encl (10) MTSA Facility Compliance Guide, CH-1
Encl (11) Additional Policy Guidance, CH-1

Table of Contents

Implementation Guidance for the Regulations Mandated by the Maritime Transportation Security Act of 2002 (MTSA) for Facilities

Enclosure 1
Plan Review Guidance Flowchart


SUBMISSION TO NATIONAL REVIEW CENTER
SUBMISSION TO COTP
Facility submits FSP to Center. Date Stamp plan.
FSP Submission may follow either path
Facility submits FSP to cognizant COTP. Date stamp plan.
COTP forwards FSP to Center.
Is Plan Required?
Yes
No
Begin Review Process
Plan Returned to submitter due to non-applicability with 105 after confirming with COTP
STAGE I & II REVIEW OF FSP PLANS
Upon Receipt, ensure Facility exists in MISLE. Create Facility & FIN as necessary. Open Plan Review Sub-Activity.
Mail FSP submitter letter acklowledging receipt of plan including FIN and Acitivity number, and instructions on how to access FSP database on CG MIX website.
Plan received after 31 Dec 2003?
Yes
Plans will be reviewed in the order received
No
FSP revisions completed
Contractor Conducts Stage 1 & 2 Plan Review w/CG oversight
Is Plan Acceptable?
No
Plan returned to facility w/comments. Plan submitter has XX days to complete revisions.
Plan Returned to Contractor with cover letter listing deficiencies
FSPs returned to cognizant COTPs. MISLE Activity updated.
Yes
STAGE III COTP REVIEW
FSP revisions completed
COTP conducts Stage III Verification Plan Review iaw guidance
Yes
Letter detailing necessary revisions mailed to Plan Submitter. Plan submitter has XX days to complete revisions. MISLE Acitivity status changed.
No
Are major revisions to plan necessary?
Is a Letter of Authorization Appropriate?
No
Stage III Plan Review Satisfactory?
Yes
Consider Enforcment Options following 1 July 2004
No
Yes
Issue Letter of Authorization to facility owner of limited duration
COTP issues Approval Letter to Plan Submitter. Closes MISLE Plan Review Acitivity.
Plan Review Complete.
IMPLEMENTATION OF INSPECTION CYCLES
Initiate Annual Inspection cycle
Implement 5 Year Security Plan Review Cycle.
Implement 5-Year Exercise Oversight Cycle.
The annual inspection cycle consists of all of the following inspections (as applicable)
-MTSA Compliance Exam
-Pollution Prevention Regs / Safety Exam (33 CFR 126, 127, 154)
-Marpol Annex I
-Marpol Annex II
-Marpol Annex V
-Marpol Annex VI

ENCLOSURE 2
MTSA FSP/ASP IMPLEMENTATION PROCESS METHODOLOGY

2.1 Enclosure Contents

2.1.1. This enclosure contains information relating to the following subject matter areas:

2.2 Definitions

2.2.1. **Letter of Approval**. A Letter of Approval is issued by the COTP to facilities satisfactorily completing Stage III review by 1 July 2004.

2.2.2. **Letter of Authorization**. A Letter of Authorization to operate is issued in lieu of a Letter of Approval. A facility to which this letter is issued meets the requirements found in 33 CFR 105.120(b). This letter is issued by the COTP to facilities meeting the following criteria:

- For existing facilities with plans that have not completed Stage III review by 1 July 2004 and with the following conditions:
    - Plan was submitted by 31 December 2003, and
    - The facility owner has met all plan correction deadlines
- For facilities not in service by 31 December 2003 that have submitted a plan no later than 60 days prior to beginning operations.
- A Letter of Authorization is cancelled once a Letter of Approval is issued or the time specified has lapsed, whichever occurs sooner.
- A Letter of Authorization shall be valid for no longer than one year.

A COTP may issue a Letter of Authorization to those facilities not meeting the above criteria on a case-by-case basis. This allows some discretion in enforcement options following 1 July 2004.

2.3 Implementation Methodology

2.3.1. The implementation of the Act's[1] requirements found in 33 CFR Part 105 will be executed in three distinct phases as outlined below. This "phased-in" methodology allows for rapid deployment of critical regulatory provisions.

2.3.2. **FSP Development and Submission Phase** (through 31 December 2003) - Key components of this period include the following:

- Facilities to which 33 CFR Part 105 applies shall submit Facility Security Plans (FSPs) to their respective Captain of the Port (COTP) or directly to the National FSP Review Center[2]. (*See 2.5 of this enclosure*)
- COTPs shall compile a list of those facilities to which 33 CFR Part 105 applies. This will require updating facility information in MISLE[3].
- Begin Stage I and II plan review for those plans submitted during this period. Submitted FSPs will be reviewed at offices located in Overland Park, KS. FSPs will be reviewed in the order in which they are received. (*See 2.6 of this enclosure*)

2.3.3. **FSP Review and Approval Phase** (1 January 2004 through 30 June 2004) – Key components of this period include the following:

- Continue Stage I and II plan review for all submitted plans. Plan reviewers will correspond directly with plan submitters (facilities). Acceptable plans will be forwarded, with completed Stage I and II review forms, to the cognizant COTP for Stage III review. Unacceptable plans will be returned to the plan submitters for revision. (*See 2.6 of this enclosure*)
- The COTP will initiate a Stage III review after receiving an FSP with successfully completed Stage I and II reviews. This review applies local knowledge and/or on-site facility visits to validate targeted portions of the plan. Facilities successfully completing Stage III will receive an FSP approval letter from the COTP. (*See 2.7 of this enclosure*)
- In the event a FSP is not approved by 1 July 2004, the COTP may issue a Letter of Authorization to operate until the FSP is approved. (*See 2.2.2 of this enclosure*)
- The COTP will communicate with facilities identified as not having submitted an FSP as required. Civil penalty action may be warranted for those facilities not complying with plan submission requirements. (*See 2.11 of this enclosure*)

[1] Unless otherwise noted, references to the Marine Transportation Safety Act of 2002 (MTSA) regulations include all requirements of 33 CFR, Subchapter H as amended by the final rules.
[2] The "National FSP Review Center" will be referred to as the "Center" throughout this enclosure.
[3] MISLE (Marine Information for Safety and Law Enforcement) is the central computer database in which most Coast Guard activities are captured.

2.3.4 **Compliance & Verification Phase** (Commencing 1 July 2004) – Key components of this period include the following:

- All facilities must be in full compliance with 33 CFR Part 105.
- Facilities operating with a FSP must have either a Letter of Approval or a Letter of Authorization issued by the COTP. (*See 2.2 of this enclosure*)
- Facilities operating under an approved Alternative Security Program (ASP) must have a letter signed by the owner or operator stating which approved ASP they are operating under and certifying that the facility is in full compliance.
- Continue Stages I, II and III of plan review as necessary.
- Begin risk-based compliance inspection program. This compliance inspection program consists of three distinct areas: an annual compliance examination, a minimum 5-year exercise oversight, and a 5-year plan review activity. (S*ee 2.10.3 of this enclosure*)
- Civil penalty action and/or suspension of operations may be warranted for those facilities not complying with plan submission and compliance requirements. (*See 2.12 of this enclosure*)

2.4 Facility Security Plan (FSP) Review - General

2.4.1. Understanding the plan review process is critical to the successful implementation of MTSA regulations. The following is a brief discussion on each critical aspect of this process. A flow-chart of this process is contained as enclosure (1). The process itself consists of a three-stage review process. Stages I and II consist of an in-depth review of the submitted plan by Center personnel, ensuring the plan meets all regulatory requirements. The Stage III review by the COTP is designed to ensure overall adequacy of the plan and ensuring it meets the specific needs of the facility. An on-site verification may be necessary, depending on the familiarity of the plan reviewer with the specific facility. Facilities must comply with their security plan by 1 July 2004 or risk enforcement actions which may include suspension of operations until compliance is reached.

2.5 Facility Security Plan Submissions

2.5.1. In accordance with reference (c), all facilities to which this part applies must submit Facility Security Plans to the cognizant COTP by 31 December 2003. As the preferred method, facilities may submit their plans directly to:

National FSP Review Center
Mailstop Q6
Attn: Security Officer
6601 College Boulevard
Overland Park, KS 66211
1-866-377-8724
1-866-FSP-USCG

2.5.2. Immediately upon receipt, the COTP shall forward all received plans to the Center utilizing an express courier service and shall log the courier's tracking number for future

reference. The plans should also be date stamped upon receipt. COTPs shall forward plans received in accordance with COMDTINST 5510.5 and shall e-mail the Center at NFSPRC@bv.com to indicate that a plan has been mailed. The e-mail will contain the following information:

- Name of Facility Plan
- Express Courier used and tracking number
- Date mailed to Center
- Unit name and point of contact
- Facility Identification Number (FIN)
- Unit OPFAC

2.5.3. Center personnel will screen all plans upon receipt to determine applicability to 33 CFR Part 105 and will review only those as required by that part. Center personnel **will** consult with the COTP before determining the regulations do not apply to a specific submission and returning the plan to the submitter. Enclosure (8) provides additional policies to define an individual facility's regulated areas.

2.6 Stage I and II Review of FSPs

2.6.1. Following a successful "applicability" determination, Center personnel will create a Plan Review Sub-Activity within MISLE. MISLE information will be audited to ensure database integrity through a review of the Facility Identification Number (FIN)[4] and PARTICULARS[5] tables. In the case that a FIN does not exist, one will be assigned.

2.6.2. After the successful completion of MISLE activities, a letter will be mailed to the plan owner and COTP containing:

- A statement acknowledging receipt of their plan;
- The unique Activity Number for their plan review activities;
- Detailed instructions on how to access the Coast Guard Marine Information Exchange (CGMIX) website and check the status of their plan; and
- MTSA FSP customer service center contact information. A sample plan receipt letter is contained as a part of enclosure (7).

2.6.3. Plans will then be screened to determine whether they were submitted by the 31 December 2003, deadline as stated in the regulations. Plans that were postmarked on or before this date will have met this requirement and will continue through the process without interruption. All plans will be reviewed in the order received, regardless.

2.6.4. Following a successful applicability screening, a plan will undergo a Stage I review to ensure the eighteen basic required sections are properly included/addressed. Center personnel will utilize the review form incorporated as enclosure (3). Major deficiencies noted during Stage

[4] Each facility has an individual and unique Facility Identification Number in MISLE. Facilities not previously regulated by the Coast Guard, but to which MTSA apply, may not currently have a FIN.
[5] Specific information for each facility is recorded in this MISLE table.

I review will require the plan to be resubmitted with corrections prior to Stage II review. Major deficiencies include the following:

- Two or more incomplete FSP content requirements[6],
- An incomplete or missing FSA report, or
- An incomplete or missing Facility Vulnerability and Security Measures Summary (CG-6025).

Center personnel will use the procedures listed in paragraph 2.6.6. of this enclosure when returning plans for corrections.

2.6.5. Following a successful Stage I review, a Stage II review will be conducted. This review assesses the plan's compliance with all regulatory requirements contained in 33CFR105. The review form is incorporated as enclosure (4). Most Stage I and II reviews will be conducted at the Center in Overland Park, KS; however, some plans may be forwarded to a regional review office. For instance, due to the unique nature of barge fleeting operations, the Houston Review Office is staffed to review all FSPs of this type. This allows for a certain specialization and, more important, consistency in the review process.

2.6.6. To expedite reviews, plans will not be returned for revisions. Instead, plan owners will receive a letter from the Center identifying deficiencies and the timeframe for submitting revisions. Sample letters are included in enclosure (7).

2.7 <u>Stage III COTP Review and Approval of FSPs</u>

2.7.1. Following a successful Stage II review, all FSPs will be mailed to the cognizant COTP for Stage III review and approval. The COTP will also receive copies of:

- Completed Stage I and II review forms,
- all correspondence between the plan submitter and Center personnel, and
- a letter detailing any review form items that could not be accurately verified by Center personnel.

2.7.2. The COTP will complete a Stage III review of the FSP. The Stage III review verifies the assessment information against the physical characteristics of the facility. All carry-over items flagged by the Center during the Stage I and II review will be addressed. On-site visits to the facility may be necessary to verify information. A Stage III review form is provided as enclosure (6).

2.7.3. The COTP has two options if deficiencies are noted during the Stage III review process:

- Inform the plan submitter via letter of the noted deficiencies and the timeframe for submitting revisions or

[6] This applies to requirements 1 through 16 listed in the Stage I review form, Enclosure (3).

- return the plan to the Center for another Stage II review with a letter detailing deficiencies found.

The decision is entirely up to the COTP, but it is expected that major deficiencies noted during Stage III will require another Stage II review by the Center. Major deficiencies are those that cannot be easily corrected by the plan owner in a timely manner, or that would require significant changes or alterations to the plan mandating another Stage II review.

2.7.4. Following a successful completion of a Stage III review, the COTP shall issue an FSP Letter of Approval. The plan review process is now complete. A sample plan approval letter is contained as a part of enclosure (7). The COTP closes the MISLE Plan Review Sub-Activity and files the plan in a secure location, in accordance with SSI protocols.

2.7.5. An FSP in Stage III review not meeting all requirements will require corrective action by the FSP owner. To expedite reviews at this stage, plans will not be returned for revisions. Instead, plan owners will receive a letter from the COTP identifying deficiencies and the timeframe for submitting revisions. The COTP may issue the facility a Letter of Authorization, allowing the facility to continue to operate pending approval. A sample Letter of Authorization is contained as part of enclosure (7).

2.8 Alternative Security Program

2.8.1. An Alternative Security Program (ASP) is a generic security plan submitted by trade associations and industry groups to be used by members in good standing. These organizations submit a repeatable security program to Coast Guard Headquarters (G-MPS) for approval. See enclosure (5) for a complete explanation of this process. Members in good standing in these organizations may implement the ASP. A facility implementing an ASP is not required to submit their FSP to the Coast Guard; however, the plan owner is encouraged to send a copy of the FSP to the cognizant COTP.

2.8.2. By December 31, 2003, individual facilities will submit a letter containing the following information to either the COTP or, preferably, the Center:

- Which **approved** ASP the facility is utilizing and
- The Coast Guard Vulnerability and Security Measures Summary (CG-6025)

2.8.3. Facilities are requested to include the name of the Facility Security Officer (FSO) and their 24-hour contact phone number. These facilities are not required to submit their entire Facility Security Plan, but shall simply submit a letter with the CG-6025 and information listed above in paragraph 2.8.2.

2.8.4. Once the Center receives the information listed above, a receipt letter will be sent to the respective facility verifying receipt, as per paragraphs 2.6.1 and 2.6.2.

2.8.5. Once the Center completes the review of the submission, a copy of the information listed in 2.8.2, along with a letter indicating successful review, will be sent to the COTP. MISLE will also be utilized to track a facility's progress through this process.

2.8.6. The COTP will conduct compliance inspections of all facilities utilizing an Alternative Security Program in accordance with section 2.10 of this enclosure.

2.9 Waivers and Equivalencies

2.9.1. Waiver requests, as dictated in the regulations, will be forwarded and evaluated for approval or disapproval at Coast Guard Headquarters (G-MPS). Area, District, and COTP staffs shall develop a process to forward all waiver and equivalency requests along with recommendations to G-MPS for consideration.

2.9.2. The waiver/equivalency package should contain the request, any submitted reference material, and a staff recommendation.

2.9.3. Upon receiving the request, G-MPS will generate a receipt letter to the originator that includes direction to continue developing the FSP pending the results of the review process.

2.9.4. Upon approval or disapproval of the waiver and/or equivalency request, the submitter will be notified by letter with the Center and the COTP receiving a copy.

2.9.5. Facilities should maintain any approved waivers and equivalencies on file with their FSP. These will also be available to the Coast Guard through MISLE.

2.10 Implementation of Inspection Cycles

2.10.1. Coast Guard personnel will continue to examine/inspect facilities on an annual basis. While implementation of the new regulations imposes numerous additional security measures that must be verified, it is the intention of the Coast Guard to maintain our current facility inspection/examination policies in regards to on-site examinations. The new requirements will be verified by Coast Guard personnel on an annual basis in conjunction with other required examinations. There are three pathways to verification following the implementation beginning on 1 July 2004. These include compliance examinations, exercise oversights and plan reviews.

2.10.2. Beginning 1 July 2004, Coast Guard personnel will enforce and verify all new security requirements during annual facility exams. These exams may verify compliance with the following regulatory requirements (as applicable):

- MTSA (33 CFR Parts 101, 103, 105)
- Pollution Prevention / Safety (33 CFR Parts 126, 127, 154)
- MARPOL Annex I, II, V, VI[7] (33 CFR Part 158)

[7] MARPOL Annex VI has not been ratified by the United States at the time of publishing this NVIC.

2.10.3. Annual security examinations will measure compliance with requirements in 33 CFR Parts 101, 103 and 105. These examinations will specifically audit a facility's compliance with their approved FSP. G-MOC is currently developing a compliance inspection form that will serve as further guidance. This form will be provided to all Coast Guard facility inspectors to ensure consistency during these examinations. COTPs will utilize a risk-based approach to determine priorities when scheduling compliance exams. COTP's are expected to schedule these compliance inspections taking into account all of the following tools/criteria:

- Port Security Risk Assessment Tool (PS-RAT) results utilizing overall facility Risk Score/Rating,
- Facility inspection history (past deficiencies/violations),
- Facility inspection cycle/schedule, and
- Economy of personnel resources.

While it is expected that COTPs will conduct compliance inspections commencing immediately after July 1, 2004 for those highest risk facilities as denoted in the PS-RAT, they may use discretion by taking into account the timing of the facilities' most recent annual inspections and deficiency histories. As an example, a COTP may schedule a compliance exam later in the period to coincide with other required facility inspections (e.g. MARPOL, 33 CFR Parts 126, 127, 154).

2.10.4. FSP approval letters are only valid for a 5-year period. Prior to letter expiration dates, facilities are required to complete a new review and approval process. This review and approval process is currently under development. Future reviews will be completed at the local COTP level.

2.10.5. The Coast Guard will also periodically monitor the required annual exercises as required by reference (c). COTPs will utilize a risk-based approach to determine the frequency of exercise oversight activities.

2.11 Enforcement Strategies - Plan Submission

2.11.1. COTPs are encouraged to use all available outreach and administrative controls at their disposal to ensure compliance with the facility security plan submittal requirements.

2.11.2. 33 CFR 105.115(a) states that on or before 31 December 2003, facility owners or operators must submit their required documents to the cognizant COTP or the Center.

2.11.3. 33 CFR 101.415 allows for a civil penalty of not more than $25,000 for any person who does not comply with the submission requirements.

2.12 Enforcement Strategies – Post 1 July 2004

2.12.1. COTPs are encouraged to use all available outreach and administrative controls at their disposal to ensure compliance with the facility in accordance with all requirements of 33 CFR Part 105.

2.12.2. 33 CFR 105.115(b) states that on or before 1 July 2004, each facility owner or operator must be operating in full compliance with 33 CFR Part 105.

2.12.3. 33 CFR 101.415 allows for a civil penalty of not more than $25,000 for any person who does not comply with any requirement of this part. In addition, this part allows for one or more of the following:

- Restriction on facility access
- Conditions on facility operations
- Suspension of facility operations
- Lesser administrative and corrective measures
- Suspension or revocation of security plan approval, thereby prohibiting a facility from operating

2.13 MISLE Methodologies

2.13.1. Enhancements have been made to the Marine Information for Safety and Law Enforcement (MISLE) database to assist in tracking the progress of a FSP through the plan review process and more accurately capture inspection types. A consolidated list of MISLE changes and newly developed data entry methodologies will be made available to COTPs through separate correspondence.

2.13.2. COTPs will be able to assess the compliance of their facilities with these requirements through use of the MISLE Analysis and Reporting System (MARS) program. MARS is a Coast Guard intranet-based program that allows users to retrieve data from the MISLE database utilizing a large number of search parameters. Guidance on MARS use will be made available to COTPs through separate correspondence.

2.14 Facility Vulnerability and Security Measures Summary (Form CG-6025)

2.14.1. Completion of the Facility Vulnerability and Security Measures Summary (Form CG-6025) is critical to summarize a facility's vulnerabilities and the security measures used to mitigate them. COTPs will use this information to aid in the development of Area Maritime Security Plans and to audit FSP implementation, recognizing that there can be multiple vulnerabilities to a facility that, while they may have a negative economic impact, may not have a significant security impact. Facility owners are requested to complete CG-6025 with a focus on the highest-risk and consequence vulnerabilities. This can be achieved by using the nine vulnerability categories listed in the key to the Form. Facility owners/operators should complete the Form for each of these nine vulnerability categories. If there is more than one vulnerability issue under the same category, list them; however, curtail the list to approximately three of the most important entries for the category. If a vulnerability category does not apply, note this fact on the Form. During the Stage III process, COTP's will review the CG-6025 and, if appropriate, suggest additional entries.

ENCLOSURE 3
STAGE 1 - USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST

Sensitive Security Information (When filled out)
United States Coast Guard

STAGE 1 - USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST

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

FSP Content Requirements:	*Yes*	*No*
Does the plan follow the order as it appears below?	☐	☐
If no, does the plan contain an index identifying the required elements and their location?	☐	☐
(1) Security administration and organization of the facility *Does the plan contain a security organization?*	☐	☐
(2) Personnel training *Does the plan contain personnel training procedures?*	☐	☐
(3) Drills and exercises *Does the plan contain drill and exercise procedures?*	☐	☐
(4) Records and documentation *Does the plan contain facility recordkeeping and documentation procedures?*	☐	☐
(5) Response to change in MARSEC Level *Does the plan contain procedures for responding to MARSEC level changes?*	☐	☐
(6) Procedures for interfacing with vessels *Does the plan contain procedures for interfacing with vessels?*	☐	☐
(7) Declaration of Security (DoS) *Does the plan identify DoS procedures?*	☐	☐
(8) Communications *Does the plan contain communication procedures?*	☐	☐
(9) Security systems and equipment maintenance *Does the plan contain security systems and equipment maintenance procedures?*	☐	☐
(10) Security measures for access control, including designated public access areas *Does the plan contain security measures for access control?*	☐	☐
(11) Security measures for restricted areas *Does the plan contain security measures for restricted areas?*	☐	☐
(12) Security measures for handling cargo *Does the plan identify security measures for handling cargo?*	☐	☐
(13) Security measures for delivery of vessel stores and bunkers *Does the plan address the security procedures for delivery of vessel stores and bunkers?*	☐	☐
(14) Security measures for monitoring *Does the plan identify security measures for monitoring?*	☐	☐
(15) Security incident procedures *Does the plan contain security incident procedures?*	☐	☐
(16) Audits and security plan amendments *Does the plan contain procedures for auditing and updating the plan?*	☐	☐
(17) Facility Security Assessment (FSA) report *Does the plan contain a FSA report?*	☐	☐
(18) Facility Vulnerability and Security Measures Summary (Form CG-6025) *Does the plan contain a completed CG-6025 form?*	☐	☐

Note: *If two or more of the above questions are marked "no," then the FSP may be returned to the originator for correction before going to stage II review. The plan may not be approved if the FSA report or the CG-6025 form is missing.*

Sensitive Security Information (When filled out)
United States Coast Guard

STAGE 1 – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST

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

Item:	*Explanation of Deficiency:*

Comments:

ENCLOSURE 4a
STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW FORM GUIDANCE
(GENERAL FACILITIES)

General Guidance for Security Plan Preparers and Reviewers

Section 1 Security administration and organization of the facility

This section of the plan describes the security administration of the facility, including the organizational elements responsible for security, such as the owner/operator, FSO, and facility personnel with security duties. The plan will describe in detail how the individual requirements of **33 CFR Part 105.200; 205;** and **210** are met.

Section 2 Personnel Training

This section of the plan describes how facility security personnel, including contractors, whether part-time, full-time, temporary, or permanent, obtain knowledge through training, or through equivalent job experience. The plan shall describe in detail how these individuals are trained in the topics provided in **33 CFR Part 105.215(a)-(e).**

Section 3 Drills and Exercises

This section of the plan describes how drills and exercises are conducted at the facility including frequency and types outlined in their FSP. The plan shall describe in detail how the individual drills and exercises are conducted as provided in **33 CFR Part 105.220.**

Section 4 Records and Documentation

This section of the plan will describe the method that is to be used to accomplish facility record keeping requirements in **33 CFR Part 105.225.**

Section 5 Response to Change in MARSEC Level

This section of the plan describes how the owner/operator will ensure facility operations reflect the security requirements for the MARSEC level in effect. The plan should describe in detail MARSEC level, coordination and implementation as described in **33 CFR Part 105.230.**

Section 6 Procedures for Interfacing with Vessels

This section of the plan describes procedures for interfacing with vessels at all MARSEC levels as required by **33 CFR Part 105.240.**

Section 7 Declaration of Security (DOS)

This section of the plan will include a DOS as required in 33CFR101.505. It describes how the DOS is used during the vessel/facility interface as required by **33 CFR Part 105.245.**

Section 8 Communications

This section of the plan describes how the facilities communication systems are designed to accomplish security program requirements including notification, systems and procedures for effective and continuous communications. This section will

include the process/procedures used to accomplish individual requirements provided in **33 CFR Part 105.235(a)-(d).**

Section 9 Security Systems and Equipment Maintenance

This section of the plan contains security system and equipment maintenance procedures as required by **33 CFR Part 105.250(a)-(c).**

Section 10 Security Measures for Access Control, including designated public access areas

This section of the plan implements general security measures for access control at all MARSEC levels. This section describes in detail the security measures required by **33 CFR Part 105.255.**
NOTE: A MARSEC Directive could affect the performance standards contained this section.

Section 11 Security Measures for Restricted Areas.

This section of the plan will contain policy for restricted areas and should include the designation and general security measures for these restricted areas at all MARSEC levels. This section should describe in detail the security measures required by **33 CFR Part 105.260.** *NOTE: A MARSEC Directive could affect the performance standards contained this section.*

Section 12 Security Measures for Handling Cargo

This section of the plan must include general security measures for cargo handling at all MARSEC levels. This section describes in detail the security measures required by **33 CFR Part 105.265.** *NOTE: a MARSEC Directive could affect the performance standards contained this section.*

Section 13 Security Measures for Delivery of Vessel Stores and Bunkers

This section of the plan must include general security measures for delivery of vessel stores and bunkers at all MARSEC levels. This section describes in detail the security measures provided in **33 CFR Part 105.270.** *NOTE: a MARSEC Directive could affect the performance standards contained this section.*

Section 14 Security Measures for Monitoring

This section of the plan implements general security measures for monitoring at all MARSEC levels. This section will describe in detail the security measures required by **33 CFR Part 105.275**. *NOTE: a MARSEC Directive could affect the performance standards contained this section.*

Section 15 Security Incident Procedures

This section of the plan will include security incident procedures for each MARSEC level. This section describes in detail the security incident procedures required by **33 CFR Part 105.280(a)-(e).**

Section 16 Audit and Security Plan Amendments

This section of the plan details how changes/amendments are made and audits are conducted at the facility. The plan will describe in detail the frequency and types, and how the amendments and audits are performed as required by **33 CFR Part 105.415.**

Section 17 Facility Security Assessment (FSA) Report

This section of the plan contains written documentation of the FSA that is based on a collection of background information, the completion of an on-scene survey and an analysis of that information for the facility. An FSA report describes in detail the individual plan requirements in **33 CFR Part 105.300; 305 and 310.**

Section 18 Facility Vulnerability and Security Measures Summary (Form CG-6025)

This is a required form that provides vulnerability and mitigating security measures for the facility as identified in the FSA. This form located in **Appendix A to Part 105.** Enclosure (2) to NVIC 03-03 contains further information on completing this form.

Additional Requirements

Additional Requirements for Passenger and Ferry Facilities

33 CFR Part 105.285 provides additional requirements for passenger and ferry facilities at all MARSEC levels. *NOTE: a MARSEC Directive could affect the performance standards contained these requirements.*

Additional Requirements for Cruise Ship Terminals

33 CFR Part 105.290 provides additional requirements for cruise ship terminals at all MARSEC levels. *NOTE: a MARSEC Directive could affect the performance standards contained these requirements.*

Additional Requirements for CDC Facilities

33 CFR Part 105.295 provides additional requirements for CDC facilities at all MARSEC levels. *NOTE: a MARSEC Directive could affect the performance standards contained these requirements.*

Additional Requirements for Barge Fleeting Facilities

33 CFR Part 105.296 provides additional requirements for barge fleeting facilities at all MARSEC levels. *NOTE: a MARSEC Directive could affect the performance standards contained these requirements.*

ENCLOSURE 4b
STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW FORM
(GENERAL FACILITIES)

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

Reviewer: _____QA Reviewer:_____ MISLE Activity #: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
(1) Security administration and organization of the facility				
105.200 Owner or operator				
1. Does the FSP include the following:				
1.1 A defined security organizational structure that identifies specific security duties and responsibilities.	☐	☐	☐	☐
1.2 FSO designation in writing with a 24-hour contact method.	☐	☐	☐	☐
1.3 Procedures for coordinating security issues between the facility and vessels.	☐	☐	☐	☐
1.4 Procedures to ensure coordination of shore leave for vessel personnel or crew change-out, identified in the plan and communicated with vessel operators in advance of a vessel's arrival.	☐	☐	☐	☐
1.5 Procedures for implementing **MARSEC Level** security measures, within 12 hours of notification of an increase.	☐	☐	☐	☐
1.6 Procedures for reporting breaches of security and security incidents (to the National Response Center).	☐	☐	☐	☐
1.7 If not in order prescribed in 33 CFR Part 105.405 (a) (1-18), is there an index or cross reference which describes the location of each section.	☐	☐	☐	☐
105.205 Facility Security Officer (FSO)				
1. General				
1.1 Does the FSP ensure that the FSO retains designated responsibilities although other individuals may perform specific tasks?	☐	☐	☐	☐
1.2 If the same person serves as the FSO for more than one facility, does the FSP identify the facility/facilities for which the FSO is designate?	☐	☐	☐	☐
1.3 If the same FSO has been identified for facilities over 50 miles apart or in different COTP zones, has a waiver been approved? *[Note: If this is applicable then Stage III Review is required for verification].*	☐	☐	☐	☐
2. Qualifications				
2.1 Does the FSP identify the following FSO responsibilities:				
2.1.1 Ensuring the Facility Security Assessment (FSA) is conducted.	☐	☐	☐	☐
2.1.2 Ensuring development and implementation of a FSP.	☐	☐	☐	☐
2.1.3 Ensuring annual audit program is implemented and maintained at the facility.	☐	☐	☐	☐
2.1.4 Ensuring FSP is exercised per Sec. 105.220 of this part.	☐	☐	☐	☐
2.1.5 Ensuring regular security inspections of the facility are conducted.	☐	☐	☐	☐
2.1.6 Ensuring security communication program includes a method to ensure that all employees and visitors are aware of security procedures.	☐	☐	☐	☐
2.1.7 Ensuring adequate training to personnel performing facility security duties.	☐	☐	☐	☐
2.1.8 Ensuring that occurrences that threaten the security of the facility are recorded and reported to the owner or operator.	☐	☐	☐	☐
2.1.9 Ensuring the maintenance of records required by this part.	☐	☐	☐	☐

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
2.1.10 Ensuring the preparation and the submission of any reports as required by this part.	☐	☐	☐	☐
2.1.11 Ensuring the execution of any required Declarations of Security with Vessel Security Officers.	☐	☐	☐	☐
2.1.12 Ensuring the coordination of security services in accordance with the approved FSP.	☐	☐	☐	☐
2.1.13 Ensuring that security equipment is properly operated, tested, calibrated, and maintained.	☐	☐	☐	☐
2.1.14 Ensuring the recording and reporting of attainment changes in **MARSEC Levels** to the owner or operator and the cognizant COTP.	☐	☐	☐	☐
2.1.15 When requested, ensure that the Vessel Security Officers receive assistance in confirming the identity of visitors and service providers seeking to board the vessel through the facility.	☐	☐	☐	☐
2.1.16 Ensuring notification, as soon as possible, to law enforcement personnel and other emergency responders to permit a timely response to any transportation security incident.	☐	☐	☐	☐
2.1.17 Ensuring that the FSP is submitted to the cognizant COTP for approval, as well as any plans to change the facility or facility infrastructure prior to amending the FSP.	☐	☐	☐	☐
2.1.18 Ensuring that all facility personnel are briefed of changes in security conditions at the facility.	☐	☐	☐	☐
105.210 Facility personnel with security duties				
1. Does the FSP identify a record keeping process to ensure that facility personnel responsible for security duties have knowledge, through appropriate training or equivalent job experience? This may include a portion or all of the following topics: 1.1 Knowledge of current security threats and patterns; 1.2 Recognition and detection of dangerous substances and devices; 1.3 Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; 1.4 Techniques used to circumvent security measures; 1.5 Crowd management and control techniques; 1.6 Security related communications; 1.7 Knowledge of emergency procedures and contingency plans; 1.8 Operation of security equipment and systems; 1.9 Testing, calibration, and maintenance of security equipment and systems; 1.10 Inspection, control, and monitoring techniques; 1.11 Relevant provisions of the Facility Security Plan (FSP); 1.12 Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores; 1.13 The meaning and the consequential requirements of the different **MARSEC Levels**.	☐	☐	☐	☐

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC Number: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
(2) Personnel training **105.215 Security training for all other facility personnel** 1. Does the FSP identify procedures or policies to ensure personnel, including contractors, whether part-time, full-time, temporary, or permanent, have knowledge of, through training or equivalent job experience, in the following as appropriate: 1.1 Relevant provisions of the Facility Security Plan (FSP); 1.2 The meaning and the consequential requirements of the different MARSEC Levels as they apply to them, including emergency procedures and contingency plans; 1.3 Recognition and detection of dangerous substances and devices; 1.4 Recognition of characteristics and behavioral patterns of persons who are likely to threaten security; 1.5 Techniques used to circumvent security measures.	☐	☐	☐	☐
(3) Drills and exercises **105.220 Drill and exercise requirements** 1. General 1.1 Does the FSP identify drills and exercises for testing the proficiency of facility personnel in assigned security duties at all **MARSEC Levels** and validate the effective implementation of the FSP?	☐	☐	☐	☐
1.2 Does the FSP direct the Facility Security Officer (FSO) to identify related security deficiencies identified during drills and exercise?	☐	☐	☐	☐
2. Drills 2.1 Does the FSO ensure at least one security drill is conducted every 3 months? (Where appropriate, security drills may be held in conjunction with non-security drills.)	☐	☐	☐	☐
2.2 Have drills tested individual elements of the FSP, including response to security threats and incidents? (Drills should account for the types of operations of the facility, facility personnel changes, the type of vessel the facility is serving, and other relevant circumstances. Examples of drills include unauthorized entry to a restricted area, response to alarms, and notification of law enforcement authorities.)	☐	☐	☐	☐
2.3 If a vessel is moored at the facility on the date the facility has planned to conduct any drills, has the facility identified that the vessel or vessel personnel are not required to be a part of or participate in the facility's scheduled drill?	☐	☐	☐	☐
3. Exercises 3.1 Does the FSP require exercises must be conducted at least once each calendar year, with no more than 18 months between exercises. (Note: Exercises may be: Full scale or live, tabletop simulation or seminar combined with other appropriate exercises, and any combination of these elements.)	☐	☐	☐	☐
3.2 Does the FSP identified exercise test communication and notification procedures, and elements of coordination, resource availability, and	☐	☐	☐	☐

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
response?				
3.3 Does the FSP identify exercises that test the entire security program and include substantial and active participation of FSOs?	☐	☐	☐	☐
(4) Records and documentation				
105.225 Facility recordkeeping requirements				
1. Does the FSP direct the FSO to keep records of the activities as set out in paragraph 2 of this section [33 CFR Part 105.225 (b)] for at least 2 years and make them available to the Coast Guard upon request?	☐	☐	☐	☐
2. Does the FSP detail that records be protected against unauthorized deletion, destruction, or amendment?				
Have procedures been identified to maintain the following records:				
2.1 Training. For each security training session, the date of each session, duration of session, a description of the training, and a list of attendees;	☐	☐	☐	☐
2.2 Drills and exercises. For each drill or exercise, the date held, description of drill or exercise, list of participants, and any best practices or lessons learned which may improve the FSP;	☐	☐	☐	☐
2.3 Incidents and breaches of security. For each incident or breach of security, the date and time of occurrence, location within the facility, description of incident or breaches, to whom it was reported, and description of the response;	☐	☐	☐	☐
2.4 Changes in **MARSEC Levels**. For each change in **MARSEC Level**, the date and time of notification received, and time of compliance with additional requirements;	☐	☐	☐	☐
2.5 Maintenance, calibration, and testing of security equipment. For each occurrence of maintenance, calibration, and testing, record the date and time, and the specific security equipment involved;	☐	☐	☐	☐
2.6 Security threats. For each security threat, the date and time of occurrence, how the threat was communicated, who received or identified the threat, description of threat, to whom it was reported, and description of the response;	☐	☐	☐	☐
2.7 Declaration of Security (DoS) A copy of each single-visit DoS and a copy of each continuing DoS for at least 90 days after the end of its effective period; and	☐	☐	☐	☐
2.8 Annual audit of the FSP. For each annual audit, a letter certified by the FSO stating the date the audit was completed.	☐	☐	☐	☐
3. Does the FSP include procedures to protect records from unauthorized access or disclosure?	☐	☐	☐	☐
4. If any approved waivers or equivalency have been identified in the FSP, then follow on identification is required in stage 3.	☐	☐	☐	☐
(5) Response to change in MARSEC Level				
105.230 Maritime Security (MARSEC) Level coordination and implementation				
1. Does the FSP identify procedure to ensure that the facility operates in	☐	☐	☐	☐

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC Number: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
compliance with the security requirements for the **MARSEC Level** in effect for the port?				
2. When notified of an increase in the **MARSEC Level**, does the FSP direct the facility owner and operator to ensure that:				
2.1 Vessels moored to the facility and vessels scheduled to arrive at the facility within 96 hours of the **MARSEC Level** change are notified of the new **MARSEC Level** and the Declaration of Security is revised as necessary;	☐	☐	☐	☐
2.2 The facility complies with the required additional security measures within 12 hours;	☐	☐	☐	☐
2.3 The facility reports compliance or noncompliance to the COTP.	☐	☐	☐	☐
3. Does the FSP require, at **MARSEC Levels 2 and 3**, the Facility Security Officer inform all facility personnel about identified threats, emphasize reporting procedures and stress the need for increased vigilance.	☐	☐	☐	☐
4. Does the FSP identify procedures to inform the COTP and obtain approval prior to interfacing with a vessel or continuing operations, when not capable of operating in compliance with the FSP?	☐	☐	☐	☐
5. Does the FSP identify procedures to ensure that the facility operates in compliance with **MARSEC Level 3** requirements, including additional measures pursuant to 33 CFR Part 6, 160, or 165, as appropriate, which may include but are not limited to:	☐	☐	☐	☐
5.1 Use of waterborne security patrol;				
5.2 Use of armed security personnel to control access to the facility and to deter, to the maximum extent practical, a transportation security incident;				
5.3 Examination of piers, wharves, and similar structures at the facility for the presence of dangerous substances or devices underwater or other threats.				
(6) Procedures for interfacing with vessels				
105.240 Procedures for interfacing with vessels				
1. Does the FSP ensure that there are measures for interfacing with vessels at all **MARSEC Levels**?	☐	☐	☐	☐
(7) Declaration of Security (DoS)				
105.245 Declaration of Security (DoS)				
1. Does the FSP ensure procedures are established for requesting a DoS and for handling DoS requests from a vessel?	☐	☐	☐	☐
2. Does the FSP, at **MARSEC Level 1**, ensure a facility receiving a cruise ship or a manned vessel carrying Certain Dangerous Cargo, in bulk, comply with the following:				
2.1 Does the FSO, prior to the arrival of a vessel to the facility, ensure that the designated representatives coordinate security needs and procedures, and agree upon the contents of the DoS for the period of time the vessel is at the facility;	☐	☐	☐	☐

Sensitive Security Information (When filled out)
United States Coast Guard
STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC: _____
Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
2.2 Upon the arrival of the vessel at the facility, the FSO and Master, VSO, or their designated representative, must sign the written DoS.	☐	☐	☐	☐
3. Does the FSP require that neither the facility nor the vessel may embark or disembark passengers, transfer cargo, or vessel stores until the DoS has been signed and implemented?	☐	☐	☐	☐
4. Does the FSP at **MARSEC Levels 2 and 3** require the FSOs, or their designated representatives, of facilities interfacing with manned vessels subject to 33 CFR Part 104, sign and implement DoS's as required in 2.1 [33 CFR Part 105.245 (b)(1)] and 2.2 [33 CFR Part 105.245 (b)(2)]of this section?	☐	☐	☐	☐
5. Does the FSP at **MARSEC Levels 1 and 2** require the FSOs of facilities interfacing with the same vessels implement a continuing DoS for multiple visits?	☐	☐	☐	☐
When a continuing DoS is used, the FSP must ensure that:				
5.1 The DoS is valid for a specific **MARSEC Level**;	☐	☐	☐	☐
5.2 The effective period at **MARSEC Level 1** does not exceed 90 days;	☐	☐	☐	☐
5.3 The effective period at **MARSEC Level 2** does not exceed 30 days.	☐	☐	☐	☐
6. Does the FSP identify when the **MARSEC Level** increases beyond that contained in the DoS or the continuing DoS is void and a new DoS must be executed?	☐	☐	☐	☐
7. Does the FSP ensure a copy of all currently valid continuing DoS's be kept with the Facility Security Plan?	☐	☐	☐	☐
8. Does the FSP contain procedures to be used when the COTP requires additional DoS implementation?	☐	☐	☐	☐
(8) Communications				
105.235 Communications				
1. Does the FSP provide a means to effectively notify facility personnel of changes in security conditions at the facility?	☐	☐	☐	☐
2. Does the identified communication system and procedures allow effective and continuous communications between the facility security personnel, vessels interfacing with the facility, the cognizant COTP, and national and local authorities with security responsibilities?	☐	☐	☐	☐
3. Does the FSP identify at each active facility access point, provide a means of contacting police, security control, or an emergency operations center, by telephones, cellular phones, and/or portable radios, or other equivalent means.	☐	☐	☐	☐
4. Does the FSP ensure facility communications systems have a backup means for both internal and external communications?	☐	☐	☐	☐
(9) Security systems and equipment maintenance				
105.250 Security systems and equipment maintenance	☐	☐	☐	☐
1. Does the FSP include procedures to ensure Security systems and equipment are in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations.	☐	☐	☐	☐

Sensitive Security Information (When filled out)
United States Coast Guard
STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC Number: _____
Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
2. Does the FSP include procedures to ensure Security systems are regularly tested in accordance with the manufacturers' recommendations; noted deficiencies corrected promptly; and the results recorded as required (33 CFR Part 105.225)?	☐	☐	☐	☐
3. Does the FSP include procedures for identifying and responding to security system and equipment failures or malfunctions?				
(10) Security measures for access control **105.255 Security measures for access control** 1. Does the FSP have procedures to ensure the implementation of security measures to:				
1.1 Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;	☐	☐	☐	☐
1.2 Secure dangerous substances and devices that are authorized by the owner or operator to be on the facility; and	☐	☐	☐	☐
1.3 Control access to the facility.	☐	☐	☐	☐
2. Does the FSP ensure that:				
2.1 The restrictions or prohibitions that prevent unauthorized access are applied for each **MARSEC Level** and all means of gaining access to the facility are addressed;	☐	☐	☐	☐
2.2 The type of restriction or prohibition to be applied and the means of enforcing them are identified;	☐	☐	☐	☐
2.3 The means of identification required to allow access to the facility and for individuals and vehicles to remain on the facility without challenge are established;	☐	☐	☐	☐
2.4 The locations where persons, personal effects and vehicle screenings are to be conducted are identified. The designated screening areas should be covered to provide for continuous operations regardless of the weather conditions.	☐	☐	☐	☐
3. Does the FSP ensure that a system is established for checking the identification of facility personnel or other persons seeking access to the facility that:				
3.1 Allows identification of authorized and unauthorized persons at any **MARSEC Level**;	☐	☐	☐	☐
3.2 Is coordinated, when practicable, with identification systems of vessels or other transportation conveyances that use the facility;	☐	☐	☐	☐
3.3 Is updated regularly;	☐	☐	☐	☐
3.4 Uses disciplinary measures to discourage abuse;	☐	☐	☐	☐
3.5 Allows temporary or continuing access for facility personnel and visitors, including seafarers' chaplains and union representatives, through the use of a badge or other system to verify their identity; and	☐	☐	☐	☐
3.6 Allows certain long-term, frequent vendor representatives to be treated more as employees than as visitors.	☐	☐	☐	☐
4. Does the FSP establish the frequency of application of access controls, particularly if they are to be applied on a random or occasional basis?	☐	☐	☐	☐
5. Does the FSP at **MARSEC Level 1** ensure the following security measures are				

Sensitive Security Information (When filled out)
United States Coast Guard
STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC: _____
Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
implemented at the facility:				
5.1 Screen persons, baggage (including carry-on items), personal effects, and vehicles, including delivery vehicles for dangerous substances and devices at the rate specified in the approved FSP, excluding government-owned vehicles on official business when government personnel present identification credentials for entry;	☐	☐	☐	☐
5.2 Conspicuously post signs that describe security measures currently in effect and clearly state that:				
5.2.1 Entering the facility is deemed valid consent to screening or inspection;	☐	☐	☐	☐
5.2.2 Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter;	☐	☐	☐	☐
5.3 Check the identification of any person seeking to enter the facility, including vessel passengers and crew, facility employees, vendors, personnel duly authorized by the cognizant authority, and visitors. This check includes confirming the reason for entry by examining at least one of the following:				
5.3.1 Joining instructions;	☐	☐	☐	☐
5.3.2 Passenger tickets;	☐	☐	☐	☐
5.3.3 Boarding passes;	☐	☐	☐	☐
5.3.4 Work orders, pilot orders, or surveyor orders;	☐	☐	☐	☐
5.3.5 Government identification; or	☐	☐	☐	☐
5.3.6 Visitor badges issued in accordance with an identification	☐	☐	☐	☐
5.3.7 System required in paragraph 3 of this section [33 CFR Part 105.255(c)];	☐	☐	☐	☐
5.4 Deny or revoke a person's authorization to be on the facility if the person is unable or unwilling, upon the request of facility personnel, to establish his or her identity or to account for his or her presence. Any such incident must be reported in compliance with this part;	☐	☐	☐	☐
5.5 Designate restricted areas and provide appropriate access controls for these areas;	☐	☐	☐	☐
5.6 Identify access points that must be secured or attended to deter unauthorized access;	☐	☐	☐	☐
5.7 Deter unauthorized access to the facility and to designated restricted areas within the facility;	☐	☐	☐	☐
5.8 Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel;	☐	☐	☐	☐
5.9 Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between the facility and a vessel.	☐	☐	☐	☐
6. Does the FSP at **MARSEC Level 2** in addition to the security measures required for **MARSEC Level 1**, ensure the implementation of additional security measures which may include as applicable:				
6.1 Increasing the frequency and detail of the screening of persons, baggage, and personal effects for dangerous substances and devices entering the facility;	☐	☐	☐	☐

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC Number: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
6.2 X-ray screening of all unaccompanied baggage;	☐	☐	☐	☐
6.3 Assigning additional personnel to guard access points and patrol the perimeter of the facility to deter unauthorized access;	☐	☐	☐	☐
6.4 Limiting the number of access points to the facility by closing and securing some access points and providing physical barriers to impede movement through the remaining access points;	☐	☐	☐	☐
6.5 Denying access to visitors who do not have a verified destination;	☐	☐	☐	☐
6.6 Deterring waterside access to the facility, which may include, using waterborne patrols to enhance security around the facility;	☐	☐	☐	☐
6.7 Except for government-owned vehicles on official business when government personnel present identification credentials for entry, screening vehicles and their contents for dangerous substances and devices at the rate specified for **MARSEC Level 2** in the approved FSP.	☐	☐	☐	☐
7. Does the FSP at **MARSEC Level 3** in addition to the security measures required for **MARSEC Level 1** and **MARSEC Level 2**, ensure the implementation of additional security measures which may include as applicable:				
7.1 Screening all persons, baggage, and personal effects for dangerous substances and devices;	☐	☐	☐	☐
7.2 Performing one or more of the following on unaccompanied baggage:				
7.2.1 Screen unaccompanied baggage more extensively; for example, x-raying from two or more angles;	☐	☐	☐	☐
7.2.2 Prepare to restrict or suspend handling unaccompanied baggage;	☐	☐	☐	☐
7.2.3 Refuse to accept unaccompanied baggage;	☐	☐	☐	☐
7.3 Being prepared to cooperate with responders and facilities;	☐	☐	☐	☐
7.4 Granting access to only those responding to the security incident or threat thereof;	☐	☐	☐	☐
7.5 Suspending access to the facility;	☐	☐	☐	☐
7.6 Suspending cargo operations;	☐	☐	☐	☐
7.7 Evacuating the facility;	☐	☐	☐	☐
7.8 Restricting pedestrian or vehicular movement on the grounds of the facility;	☐	☐	☐	☐
7.9 Increasing security patrols within the facility.	☐	☐	☐	☐
(11) Security measures for restricted areas				
105.260 Security measures for restricted areas				
1. Does the FSP ensure the designation of restricted areas in order to:				
1.1 Prevent or deter unauthorized access;	☐	☐	☐	☐
1.2 Protect persons authorized to be in the facility;	☐	☐	☐	☐
1.3 Protect the facility;	☐	☐	☐	☐
1.4 Protect vessels using and serving the facility;	☐	☐	☐	☐
1.5 Protect sensitive security areas within the facility;	☐	☐	☐	☐
1.6 Protect security and surveillance equipment and systems; and	☐	☐	☐	☐
1.7 Protect cargo and vessel stores from tampering.	☐	☐	☐	☐
2. Does the FSP ensure restricted areas are designated within the facility? The policy shall also ensure that all restricted areas are clearly marked and indicate				

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security (the facility owner or operator may also designate the entire facility as a restricted area.) Restricted areas must include, as appropriate:				
2.1 Shore areas immediately adjacent to each vessel moored at the facility;	☐	☐	☐	☐
2.2 Areas containing sensitive security information, including cargo documentation;	☐	☐	☐	☐
2.3 Areas containing security and surveillance equipment and systems and their controls, and lighting system controls;	☐	☐	☐	☐
2.4 Areas containing critical facility infrastructure, including:				
2.4.1 Water supplies;	☐	☐	☐	☐
2.4.2 Telecommunications;	☐	☐	☐	☐
2.4.3 Electrical system;	☐	☐	☐	☐
2.4.4 Access points for ventilation and air-conditioning systems;	☐	☐	☐	☐
2.5 Manufacturing or processing areas and control rooms;	☐	☐	☐	☐
2.6 Locations in the facility where access by vehicles and personnel should be restricted;	☐	☐	☐	☐
2.7 Areas designated for loading, unloading or storage of cargo and stores;	☐	☐	☐	☐
2.8 Areas containing cargo consisting of dangerous goods or hazardous substances, including certain dangerous cargoes.	☐	☐	☐	☐
3. Does the FSP have processes that ensure that all restricted areas have clearly established security measures to:				
3.1 Identify which facility personnel are authorized to have access;	☐	☐	☐	☐
3.2 Determine which persons other than facility personnel are authorized to have access;	☐	☐	☐	☐
3.3 Determine the conditions under which that access may take place;	☐	☐	☐	☐
3.4 Define the extent of any restricted area;	☐	☐	☐	☐
3.5 Define the times when access restrictions apply;	☐	☐	☐	☐
3.6 Clearly mark all restricted areas and indicate that access to the area is restricted and that unauthorized presence within the area constitutes a breach of security;	☐	☐	☐	☐
3.7 Control the entry, parking, loading and unloading of vehicles;	☐	☐	☐	☐
3.8 Control the movement and storage of cargo and vessel stores;	☐	☐	☐	☐
3.9 Control unaccompanied baggage or personal effects.	☐	☐	☐	☐
4. Does the FSP at **MARSEC Level 1**, ensure the implementation of security measures to prevent unauthorized access or activities within the area. These security measures may include as applicable:				
4.1 Restricting access to only authorized personnel;	☐	☐	☐	☐
4.2 Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points;	☐	☐	☐	☐
4.3 Assigning personnel to control access to restricted areas;	☐	☐	☐	☐
4.4 Verifying the identification and authorization of all persons and all vehicles seeking entry;	☐	☐	☐	☐
4.5 Patrolling or monitoring the perimeter of restricted areas;	☐	☐	☐	☐
4.6 Using security personnel, automatic intrusion detection devices, surveillance equipment, or surveillance systems to detect unauthorized	☐	☐	☐	☐

Sensitive Security Information (When filled out)
United States Coast Guard
STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC Number: _____
Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
entry or movement within restricted areas;				
4.7 Directing the parking, loading, and unloading of vehicles within a restricted area;	☐	☐	☐	☐
4.8 Controlling unaccompanied baggage and or personal effects after screening;	☐	☐	☐	☐
4.9 Designating restricted areas for performing inspections of cargo and vessel stores while awaiting loading;	☐	☐	☐	☐
4.10 Designating temporary restricted areas to accommodate facility operations. If temporary restricted areas are designated, the FSP must include a requirement to conduct a security sweep of the designated temporary restricted area both before and after the area has been established.	☐	☐	☐	☐
5. Does the FSP at **MARSEC Level 2**, in addition to the security measures required for **MARSEC Level 1** ensure the implementation of additional security measures. These additional security measures may include:				
5.1 Increasing the intensity and frequency of monitoring and access controls on existing restricted access areas;	☐	☐	☐	☐
5.2 Enhancing the effectiveness of the barriers or fencing surrounding restricted areas, by the use of patrols or automatic intrusion detection devices;	☐	☐	☐	☐
5.3 Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses;	☐	☐	☐	☐
5.4 Restricting parking adjacent to vessels;	☐	☐	☐	☐
5.5 Further restricting access to the restricted areas and movements and storage within them;	☐	☐	☐	☐
5.6 Using continuously monitored and recorded surveillance equipment;	☐	☐	☐	☐
5.7 Enhancing the number and frequency of patrols, including waterborne patrols undertaken on the boundaries of the restricted areas and within the areas;	☐	☐	☐	☐
5.8 Establishing and restricting access to areas adjacent to the restricted areas.	☐	☐	☐	☐
6. Does the FSP at **MARSEC Level 3**, in addition to the security measures required for **MARSEC Level 1** and **MARSEC Level 2**, ensure the implementation of additional security measures? These additional security measures may include as appropriate:				
6.1 Restricting access to additional areas;	☐	☐	☐	☐
6.2 Prohibiting access to restricted areas;	☐	☐	☐	☐
6.3 Searching restricted areas as part of a security sweep of all or part of the facility.	☐	☐	☐	☐
(12) Security measures for handling cargo				
105.265 Security measures for handling cargo				
1. Does the FSP ensure that security measures relating to cargo handling, some of which may have to be applied in liaison with the vessel, are implemented in order to:				
1.1 Deter tampering;	☐	☐	☐	☐
1.2 Prevent cargo that is not meant for carriage from being accepted and	☐	☐	☐	☐

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
stored at the facility without the knowing consent of the facility owner or operator;				
1.3 Identify cargo that is approved for loading onto vessels interfacing with the facility;	☐	☐	☐	☐
1.4 Include cargo control procedures at access points to the facility;	☐	☐	☐	☐
1.5 Identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up;	☐	☐	☐	☐
1.6 Restrict the entry of cargo to the facility that does not have a confirmed date for loading, as appropriate;	☐	☐	☐	☐
1.7 Ensure the release of cargo only to the carrier specified in the cargo documentation;	☐	☐	☐	☐
1.8 Coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures;	☐	☐	☐	☐
1.9 Create, update, and maintain a continuous inventory, including location, of all dangerous goods or hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods or hazardous substances;	☐	☐	☐	☐
2. Does the FSP at **MARSEC Level 1** ensure the implementation of measures to:				
2.1 Routinely check cargo, cargo transport units, and cargo storage areas within the facility prior to, and during, cargo handling operations to deter tampering;	☐	☐	☐	☐
2.2 Check that cargo, containers, or other cargo transport units entering the facility match the delivery note or equivalent cargo documentation;	☐	☐	☐	☐
2.3 Screen vehicles;	☐	☐	☐	☐
2.4 Check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility.	☐	☐	☐	☐
3. Does the FSP at **MARSEC Level 2**; in addition to the security measures required for **MARSEC Level 1** ensure the implementation of additional security measures. These additional security measures may include as applicable:				
3.1 Conducting checks of cargo, containers or other cargo transport units, and cargo storage areas within the port facility for dangerous substances and devices to the facility and vessel;	☐	☐	☐	☐
3.2 Intensifying checks, as appropriate, to ensure that only the documented cargo enters the facility, is temporarily stored there, and then loaded onto the vessel;	☐	☐	☐	☐
3.3 Intensifying the screening of vehicles;	☐	☐	☐	☐
3.4 Increasing frequency and detail in checking of seals and other methods used to prevent tampering;	☐	☐	☐	☐
3.5 Segregating inbound cargo, outbound cargo, and vessel stores;	☐	☐	☐	☐
3.6 Increasing the frequency and intensity of visual and physical inspections;	☐	☐	☐	☐
3.7 Limiting the number of locations where dangerous goods and hazardous substances, including certain dangerous cargoes, can be stored.	☐	☐	☐	☐
4. Does the FSP at **MARSEC Level 3**, in addition to the security measures required for **MARSEC Level 1** and **MARSEC Level 2**, ensure the				

Sensitive Security Information (When filled out)
United States Coast Guard
STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC Number: _____
Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
implementation of additional security measures.. These additional security measures may include as applicable:				
4.1 Restricting or suspending cargo movements or operations within all or part of the facility or specific vessels;	☐	☐	☐	☐
4.2 Being prepared to cooperate with responders and vessels;	☐	☐	☐	☐
4.3 Verifying the inventory and location of any dangerous goods and hazardous substances, including certain dangerous cargoes, held within the facility and their location.	☐	☐	☐	☐
(13) Security measures for delivery of vessel stores and bunkers				
105.270 Security measures for delivery of vessel stores and bunkers				
1. **General**				
1.1 Is there a description of security measures to prevent tampering?	☐	☐	☐	☐
1.2 Is there a description of procedures to check vessel stores for package integrity?	☐	☐	☐	☐
1.3 Is there a description of procedures to prevent vessel stores from being accepted without inspection?	☐	☐	☐	☐
1.4 Is there a description of procedures for vessels that routinely use a facility, establish and execute standing arrangements between the vessel, its suppliers, and a facility regarding notification and the timing of deliveries and their documentation?	☐	☐	☐	☐
1.5 Is there a description of procedures to check vessel stores by one of the following means:				
1.5.1 Visual examination?	☐	☐	☐	☐
1.5.2 Physical examination?	☐	☐	☐	☐
1.5.3 Detection devices, such as scanners?	☐	☐	☐	☐
1.5.4 Canines?	☐	☐	☐	☐
2. **MARSEC Level 1** – Is there a description of security measures and procedures for the delivery of vessel stores and bunkers which includes				
2.1 Screening vessel stores at the rate specified in the approved Facility Security Plan (FSP)?	☐	☐	☐	☐
2.2 Requiring advance notification of vessel stores or bunkers delivery, including a list of stores, delivery vehicle driver information, and vehicle registration information?	☐	☐	☐	☐
2.3 Screening delivery vehicles at the frequencies specified in the approved FSP?	☐	☐	☐	☐
2.4 Escorting delivery vehicles within the facility at the rate specified by the approved FSP?	☐	☐	☐	☐
3. **MARSEC Level 2** – Is there a description of security measures and procedures for the delivery of vessel stores and bunkers which includes **one or all** of the following:				
3.1 Detailed screening of vessel stores?	☐	☐	☐	☐
3.2 Detailed screening of all delivery vehicles?	☐	☐	☐	☐
3.3 Coordinating with vessel personnel to check the order against the delivery note prior to entry to the facility?	☐	☐	☐	☐

Sensitive Security Information (When filled out)
United States Coast Guard
STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC: _____
Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
3.4 Ensure delivery vehicles are escorted within the facility?	☐	☐	☐	☐
3.5 Restricting or prohibiting the entry of vessel stores that will not leave the facility within a specified period?	☐	☐	☐	☐
4. **MARSEC Level 3** – Is there a description of security measures and procedures for the delivery of vessel stores and bunkers which includes **one or all** of the following:				
4.1 Checking all vessel stores more extensively?	☐	☐	☐	☐
4.2 Restricting or suspending delivery of vessel stores?	☐	☐	☐	☐
4.3 Refusing to accept vessel stores on the facility?	☐	☐	☐	☐
(14) Security measures for monitoring				
105.275 Security measures for monitoring				
1. **General** - Is there a description of security measures that have the capability to continuously monitor, through a combination of lighting, security guards, waterborne patrols, automatic intrusion-detection devices, surveillance equipment, or any other security measures for each of the following facility features:				
1.1 Facility and its nearby approaches, on land and water?	☐	☐	☐	☐
1.2 Restricted areas within the facility?	☐	☐	☐	☐
1.3 Vessels at the facility and/or areas surrounding the vessels?	☐	☐	☐	☐
2. **MARSEC Level 1** – Is there a description of security measures and procedures for monitoring the facility which includes:				
2.1 That when automatic intrusion-detection devices are used, it activates an audible or visual alarm that is either continuously attended or monitored?	☐	☐	☐	☐
2.2 Provisions for monitoring equipment to function continually, including consideration of the possible effects of weather or of a power disruption?	☐	☐	☐	☐
2.3 Monitors the facility area, including shore and waterside access to it?	☐	☐	☐	☐
2.4 The capability of monitors access points, barriers and restricted areas?	☐	☐	☐	☐
2.5 The capability of monitors access and movements adjacent to vessels using the facility, including augmentation of lighting provided by the vessel itself?	☐	☐	☐	☐
2.6 Provisions to limit lighting effects, such as glare, and their impact on safety, navigation, and other security activities?	☐	☐	☐	☐
3. **MARSEC Level 2** – Is there a description of security measures and procedures for monitoring the facility which includes **one or all** of the following:				
3.1 Increasing the coverage and intensity of surveillance equipment, including the provision of additional surveillance coverage?	☐	☐	☐	☐
3.2 Increasing the frequency of foot, vehicle or waterborne patrols?	☐	☐	☐	☐
3.3 Assigning additional security personnel to monitor and patrol?	☐	☐	☐	☐
3.4 Increasing the coverage and intensity of lighting, including the provision of additional lighting and coverage?	☐	☐	☐	☐
4. **MARSEC Level 3** – Is there a description of security measures and procedures for monitoring the facility which includes **one or all** of the following:				
4.1 Switching on all lighting within, or illuminating the vicinity of, the	☐	☐	☐	☐

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC Number: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
facility?				
4.2 Switching on all surveillance equipment capable of recording activities within or adjacent to the facility?	☐	☐	☐	☐
4.3 Maximizing the length of time such surveillance equipment can continue to record?	☐	☐	☐	☐
4.4 A description of procedures to comply with the instructions issued by those responding to the security incident?	☐	☐	☐	☐
(15) Security incident procedures				
105.280 Security incident procedures				
1. Is there a description of procedures for responding to security threats or breaches of security and maintain critical facility and vessel-to-facility interface?	☐	☐	☐	☐
2. Is there a description of procedures for evacuating the facility in case of security threats or breaches of security, or other incidents?	☐	☐	☐	☐
3. Is there a description of procedures for reporting security incidents?	☐	☐	☐	☐
4. Is there a procedures identified for securing non-critical operations during a security incident?	☐	☐	☐	☐
(16) Audits and security plan amendments				
105.415 Amendment and audit				
1. Does the FSP identify that an audit shall be conducted on a yearly basis or when a change in ownership has occurred?	☐	☐	☐	☐
2. Is the audit process defined in the FSP?	☐	☐	☐	☐
3. Does the FSP describe who will conduct the audit?	☐	☐	☐	☐
4. Does the FSP describe the experience and knowledge levels of the person conducting the audit?	☐	☐	☐	☐
5. Does the FSP contain procedures to perform an audit when amendments have been made to FSP?	☐	☐	☐	☐
(17) Facility Security Assessment (FSA) plan amendments				
Subpart C--Facility Security Assessment (FSA)				
105.305 Facility Security Assessment (FSA) requirements				
1. Does the FSA report contain the following:				
1.1 Is there a summary of how the on-scene survey was conducted?	☐	☐	☐	☐
1.2 Is there a description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems?	☐	☐	☐	☐
1.3 Is there a description of each vulnerability found during the on-scene survey?	☐	☐	☐	☐
1.4 Is there a description of security measures that could be used to address each vulnerability?	☐	☐	☐	☐
1.5 Is there a list of the key facility operations that are important to protect?	☐	☐	☐	☐
1.6 Is there a list of identified weaknesses, including human factors, in the infrastructure, policies, and procedures of the facility?	☐	☐	☐	☐
2. Are the following elements addressed within the FSA report:				

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending Stage III*	*Not Applicable*
2.1 Physical security?	☐	☐	☐	☐
2.2 Structural integrity?	☐	☐	☐	☐
2.3 Personnel protection systems?	☐	☐	☐	☐
2.4 Procedural policies?	☐	☐	☐	☐
2.5 Radio and telecommunication systems, including computer systems and networks?	☐	☐	☐	☐
2.6 Relevant transportation infrastructure?	☐	☐	☐	☐
2.7 Utilities?	☐	☐	☐	☐
3. Is there a list of the persons, activities, services, and operations that are important to protect, in each of the following categories within the FSA report:				
3.1 Facility personnel?	☐	☐	☐	☐
3.2 Passengers, visitors, vendors, repair technicians, vessel personnel, etc?	☐	☐	☐	☐
3.3 Capacity to maintain emergency response?	☐	☐	☐	☐
3.4 Cargo, particularly dangerous goods and hazardous substances?	☐	☐	☐	☐
3.5 Delivery of vessel stores?	☐	☐	☐	☐
3.6 Any facility security communication and surveillance systems?	☐	☐	☐	☐
3.7 Any other facility security systems, if any?	☐	☐	☐	☐
4. Does the FSA report account for the vulnerabilities in the following areas:				
4.1 Conflicts between safety and security measures?	☐	☐	☐	☐
4.2 Conflicts between duties and security assignments?	☐	☐	☐	☐
4.3 The impact of watch-keeping duties and risk of fatigue on facility personnel alertness and performance?	☐	☐	☐	☐
4.4 Security training deficiencies?	☐	☐	☐	☐
4.5 Security equipment and systems, including communication systems?	☐	☐	☐	☐
5. Does the FSA report discuss and evaluate key facility measures and operations:				
5.1 Are there procedure identified to evaluate the performance of security duties?	☐	☐	☐	☐
5.2 Are there procedures identified for controlling access to the facility, through the use of identification systems or otherwise?	☐	☐	☐	☐
5.3 Are there procedures identified for controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied)?	☐	☐	☐	☐
5.4 Are there procedures identified for the handling of cargo and the delivery of vessel stores?	☐	☐	☐	☐
5.5 Are there procedures identified for monitoring restricted areas to ensure that only authorized persons have access?	☐	☐	☐	☐
5.6 Are there procedures identified for monitoring the facility and areas adjacent to the pier?	☐	☐	☐	☐
5.7 Is there readily available security communications, information, and equipment?	☐	☐	☐	☐
5.8 Are there procedures identified to protect the FSA, FSA report, and FSP from unauthorized access or disclosure?	☐	☐	☐	☐
(18) Facility Vulnerability and Security Measures Summary (Form CG-6025) **Appendix A to Part 105--Facility Vulnerability and Security Measures**				

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC Number: _____

Facility Name: _____ Facility Type: _____

FSP Content Requirements:	***Satisfactory***	***Not Satisfactory***	***Pending Stage III***	***Not Applicable***
Summary (Form CG-6025)				
1. Has Form CG-6025 been completed?	☐	☐	☐	☐
2. Are the vulnerabilities identified on Form CG-6025:				
2.1 Do the descriptions of each vulnerability identified within the FSA report correlate with the vulnerabilities identified within Form CG-6025?	☐	☐	☐	☐
2.2 Do the descriptions of security measures found within the FSA report and the FSP correlate with the security measures identified within Form CG-6025?	☐	☐	☐	☐

Sensitive Security Information (When filled out)

United States Coast Guard

STAGE II – USCG FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

Facility Identification Number: _____ OPFAC: _____

Facility Name: _____ Facility Type: _____

Item:	***Incomplete Reason:***

ENCLOSURE 5
GUIDANCE FOR SUBMISSION OF ALTERNATIVE SECURITY PROGRAM (ASP)

5.1 Enclosure Contents

5.1.1. This enclosure contains information relating to the following subject matter:

5.2 Guidance for submission of Alternative Security Programs (ASP)

5.2.1. 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 Parts 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.

5.3 Application requirements

5.3.1. 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.

5.3.2. An ASP that only addresses intended alternatives is not sufficient.

5.4 Program submission

5.4.1. 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

5.4.2. Each package must contain a:

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

5.5 Action upon receipt

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

5.5.2. 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.

5.5.3. 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.

5.5.4. 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.

5.5.5. 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.

5.6 Compliance

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

5.6.2. **Facility owner or operators** using an ASP must send their Facility Vulnerability Assessment (CG-6025) to the Coast Guard National Plan Review Center or Captain of the Port (COTP) along with a letter stating which approved ASP they are intending to use to:

National FSP Review Center
Mailstop Q6
6601 College Boulevard
Overland Park, Kansas 66211
1-866-FSP-USCG or 1-866-377-8724

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

5.6.4. **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.

5.7 Operational security

5.7.1. Security plans, including Vessel Security Plans, Facility Security Plans, and ASPs, are considered Sensitive Security Information (SSI), and therefore, 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.

5.8 Telephonic, e-mail and face-to-face inquiries

5.8.1. 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 applicability 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.

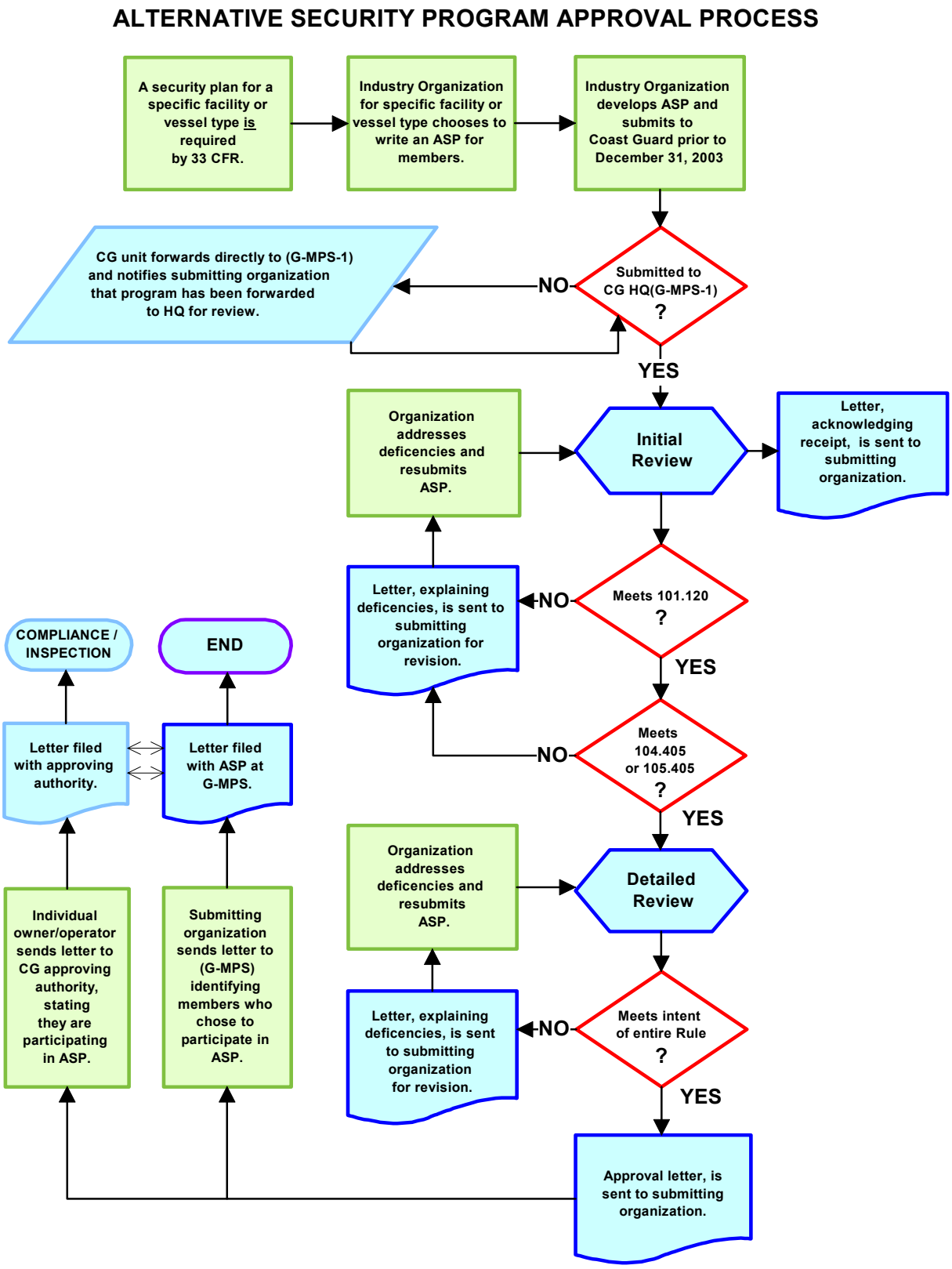

ALTERNATIVE SECURITY PROGRAM APPROVAL PROCESS
A security plan for a specific facility or vessel type is required by 33 CFR.
Industry Organization for specific facility or vessel type chooses to write an ASP for members.
Industry Organization develops ASP and submits to Coast Guard prior to December 31, 2003
Submitted to CG HQ(G-MPS-1) ?
NO
CG unit forwards directly to (G-MPS-1) and notifies submitting organization that program has been forwarded to HQ for review.
YES
Initial Review
Letter, acknowledging receipt, is sent to submitting organization.
Organization addresses deficencies and resubmits ASP.
Meets 101.120 ?
NO
Letter, explaining deficencies, is sent to submitting organization for revision.
YES
Meets 104.405 or 105.405 ?
NO
YES
Detailed Review
Organization addresses deficencies and resubmits ASP.
Meets intent of entire Rule ?
NO
Letter, explaining deficencies, is sent to submitting organization for revision.
YES
Approval letter, is sent to submitting organization.
COMPLIANCE / INSPECTION
END
Letter filed with approving authority.
Letter filed with ASP at G-MPS.
Individual owner/operator sends letter to CG approving authority, stating they are participating in ASP.
Submitting organization sends letter to (G-MPS) identifying members who chose to participate in ASP.

Figure 5-1

5.9 Guidance for submission of Equivalency Requests or Waiver Requests

5.9.1. 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).

5.10 Application requirements

5.10.1. Equivalency requests. For any security measure required by 33 CFR Parts 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 equivalency request. Each application must contain:

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

5.10.2. Waiver requests. Owners or operators are permitted to apply for a waiver of any requirement in 33 CFR Parts 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.

5.11 Request submission

5.11.1 Equivalency and 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

5.11.2. Each package must contain a:

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

5.12 Action upon receipt

5.12.1. 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.

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

5.12.3. 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.

5.12.4. Applications that pass the initial review will then undergo a detailed review. Coast Guard Headquarters (G-MPS) may request further review and input from the Area commands. 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.

5.12.5. 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.

5.12.6. 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.

5.13 Operational Security

5.13.1. 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.

5.14 Telephonic, e-mail and face-to-face inquiries

5.14.1. 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 applicability 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.

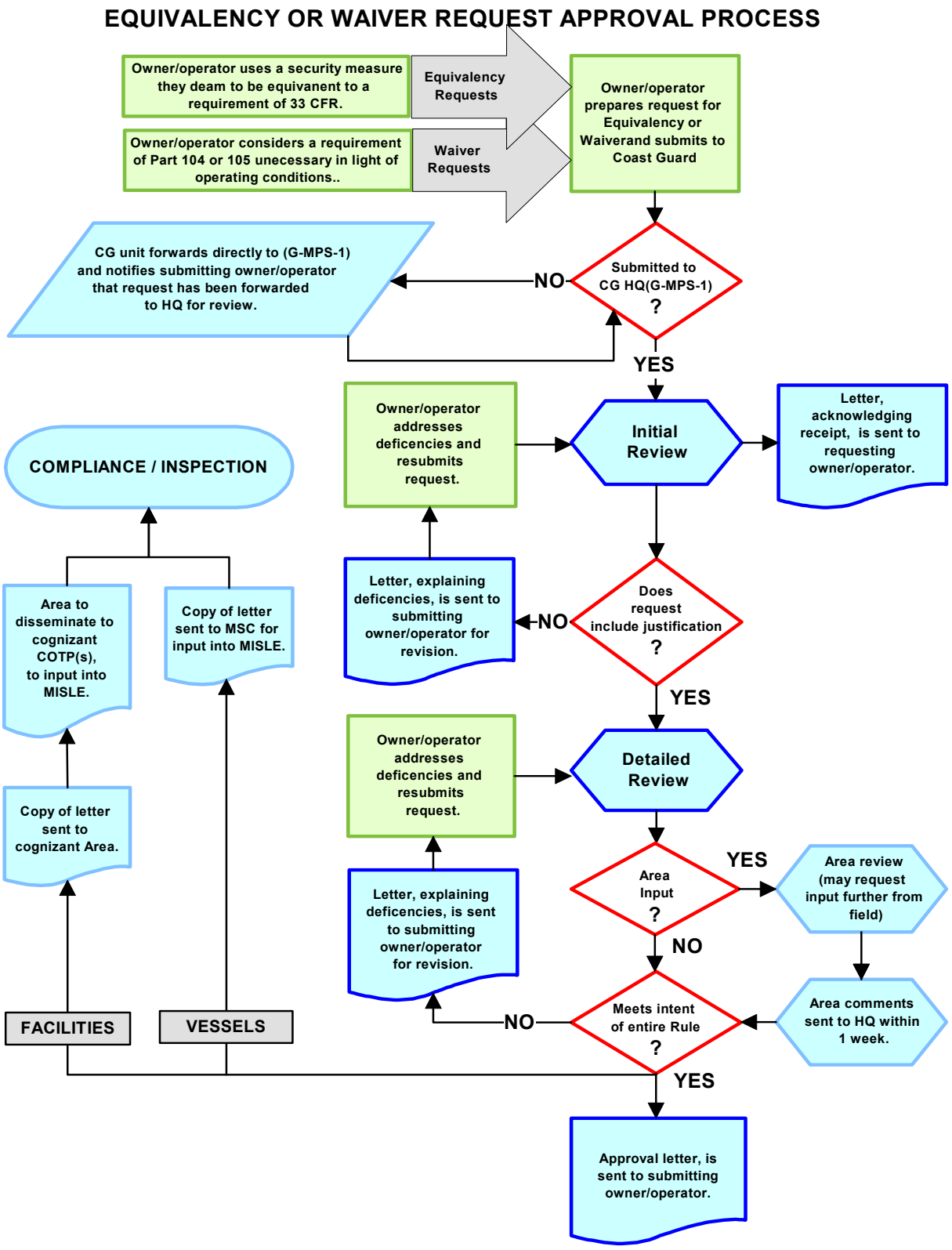

EQUIVALENCY OR WAIVER REQUEST APPROVAL PROCESS
Owner/operator uses a security measure they deam to be equivanent to a requirement of 33 CFR.
Equivalency Requests
Owner/operator considers a requirement of Part 104 or 105 unecessary in light of operating conditions..
Waiver Requests
Owner/operator prepares 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
Owner/operator addresses deficencies and resubmits request.
Letter, acknowledging receipt, is sent to requesting owner/operator.
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.
COMPLIANCE / 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

Figure 5-2

ENCLOSURE 6
STAGE III – USCG FACILITY SECURITY PLANS (FSP) APPROVAL CHECKLIST

United States Coast Guard

STAGE III – USCG FACILITY SECURITY PLANS (FSP) APPROVAL CHECKLIST

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

FSP Content Requirements:	*Complete*	*Incomplete*
(1) Review and evaluate Stage II Review form and address pending items *This may range from phone call to facility to on-site facility visit.*	☐	☐
(2) Review and evaluate Facility Security Assessment *Ensure all vulnerabilities have been identified and addressed. This may be accomplished by utilizing local knowledge or on-site surveys.*	☐	☐
(3) Obtain facility physical graphic of entire complex. *Although existing regulated 154 facilities are required to supply a physical layout of their facility, this only includes their MTRF.*	☐	☐
(4) Approval letter signed and delivered *For plans satisfactorily completing items 1-4 above (as appropriate)*	☐	☐
(5) Letter of Authorization signed and delivered *For plans not satisfactorily completing items 1-4 above (as appropriate) when plan submitters otherwise meet required deadlines.*	☐	☐

Item:	*Incomplete Reason:*

ENCLOSURE 7
SAMPLE PLAN REVIEW-RELATED LETTERS

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

Unit

Address
Staff Symbol:
Phone:
Fax:

SSIC
Date
MISLE Activity # XXXXXXX
FIN #: XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE PLAN RECEIPT LETTER

Dear Mr./Ms. XXXX:

We are in receipt of your [*Facility Security Plan*] / [*Alternate Security Program*] 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 ***To Be Determined***. 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 [*title*] [*X. X. Name*] at 1-866-FSP-USCG (1-866-377-8724).

Sincerely,

X. X. NAME
[*title*], U.S. Coast Guard
National Facility Security Plan Review Center
By direction

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

Unit

Address
Staff Symbol:
Phone:
Fax:

SSIC
Date
MISLE Activity # XXXXXXX
FIN #: XXXXX

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 *[Facility Name]*. Regrettably, your plan does not meet the requirements as outlined in 33 CFR Part 105 and is being returned for correction. Enclosed are the essential element(s) missing in your plan. These element(s) must 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, your plan will be forwarded for Stage II review.

Should you have any further questions concerning your facility security plan review, please contact [*title*] [*X. X. Name*] at 1-866-FSP-USCG (1-866-377-8724).

Sincerely,

X. X. NAME
[*title*], U.S. Coast Guard
National Facility Security Plan Review Center
By direction

Encl: (1)

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

Unit

Address
Staff Symbol:
Phone:
Fax:

SSIC
Date
MISLE Activity # XXXXXXX
FIN #: XXXXXX

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 *[Facility Name]*. Unfortunately, your plan does not meet the requirements as outlined in 33 CFR Part 105. Enclosed is a summary of the element(s) missing in your plan. These deficiencies must 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 to the cognizant Captain of the Port for approval.

Should you have any further questions concerning your facility security plan review, please contact [*title*] [*X. X. Name*] at 1-866-FSP-USCG (1-866-377-8724).

Sincerely,

X. X. NAME
[*title*], U.S. Coast Guard
National Facility Security Plan Review Center
By direction

Encl: (1)

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

Unit

Address
Staff Symbol:
Phone:
Fax:

SSIC
Date
MISLE Activity # XXXXXXX
FIN #: XXXXXX

Company Name
Address
City, State, Zip

SAMPLE LETTER OF AUTHORIZATION

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 105, 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 *[NLT October 31, 2004]*, at which time the Coast Guard will reevaluate the status and progress of your plan submission.

Commencing July 1, 2004, *[Facility Name]* must operate in full compliance with their submitted FSP and the following additional requirements [*insert requirements as appropriate*]:

You are reminded that any deviation from this submitted plan or the above additional requirements requires immediate notification to this office. Your facility security plan is sensitive security information and must be protected in accordance with 49 CFR Part 1520. A copy of your security plan and any amendments must 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

Unit

Address
Staff Symbol:
Phone:
Fax:

SSIC
Date
MISLE Activity # XXXXXXX
FIN #: 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 105, is approved.

Commencing July 1, 2004, *[Facility Name]* must operate in compliance with this approved security plan and any additional requirements contained in 33 CFR Part 105. Your facility is subject to inspections by Coast Guard personnel to verify compliance with your security plan. Failure to comply with the requirements of 33 CFR Part 105, including those as outlined in your facility security plan, may result in suspension or revocation of this security plan approval, thereby making this facility ineligible to operate in, on, under, or adjacent to waters subject to the jurisdiction of the U.S. in accordance with 46 USC 70103(c)(5). Your facility security plan is sensitive security information and must be protected in accordance with 49 CFR Part 1520. A copy of your security plan and any amendments must 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 must review your plans annually and submit any amendments to this office for re-approval as required by Title 33, CFR 105.410 and 105.415. **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

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

Unit

Address
Staff Symbol:
Phone:
Fax:

SSIC
Date
MISLE Activity # XXXXXXX
FIN #: XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE INTERIM 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 105, is approved on an interim basis. This Interim Letter of Approval will expire on *[NLT October 31, 2004]*, at which time the Coast Guard will reevaluate the status and progress of your plan submission. Your facility shall continue to work proactively with the National FSP Review Center to correct any remaining deficiencies with your security plan.

Commencing July 1, 2004, *[Facility Name]* must operate in compliance with this interim approved security plan and any additional requirements contained in 33 CFR Part 105. Your facility is subject to inspections by Coast Guard personnel to verify compliance with your security plan. Failure to comply with the requirements of 33 CFR Part 105, including those as outlined in your facility security plan, may result in suspension or revocation of this security plan approval, thereby making this facility ineligible to operate in, on, under, or adjacent to waters subject to the jurisdiction of the U.S. in accordance with 46 USC 70103(c)(5). Your facility security plan is sensitive security information and must be protected in accordance with 49 CFR Part 1520. A copy of your security plan and any amendments must be made available to Coast Guard personnel upon request.

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

ENCLOSURE 8
ADDITIONAL APPLICABILITY GUIDANCE

8.1 Applicability Job Aid

8.1.1. On 27-28 August 2003, a working group met to develop regulatory models for the application of the MTSA security regulations. This issue has proven to be difficult due to the sheer magnitude of the industry and the many different facility and operational arrangements that exist. The meeting included Coast Guard personnel from Headquarters, Area, District and COTP offices; the Environmental Protection Agency (EPA); trade associations; and industry representatives.

8.1.2. The requirements of 33 CFR 105.105 states the applicability for facilities. Under previous rules and regulations, the Coast Guard inspected to the first valve inside the secondary containment (for bulk oil and chemical facilities). The requirements of 33 CFR 105 apply not only to the waterfront facility, Marine Transportation Related (MTR) facility or Marine Transfer Area (MTA) as they are defined in 33 CFR parts 126, 127, 154, but also include areas that are contiguous, adjacent and under common owner/operators extending to the furthest security perimeter from these facilities. The following scenarios are in keeping with this interpretation. The enclosed satellite photographs and scenarios describe models applicable to bulk oil and chemical facilities. These photographs were randomly selected from publicly available resources. The scenarios developed were not intended to represent actual operations at the pictured facility. The photographs were generated to identify options for various facility arrangements that exist.

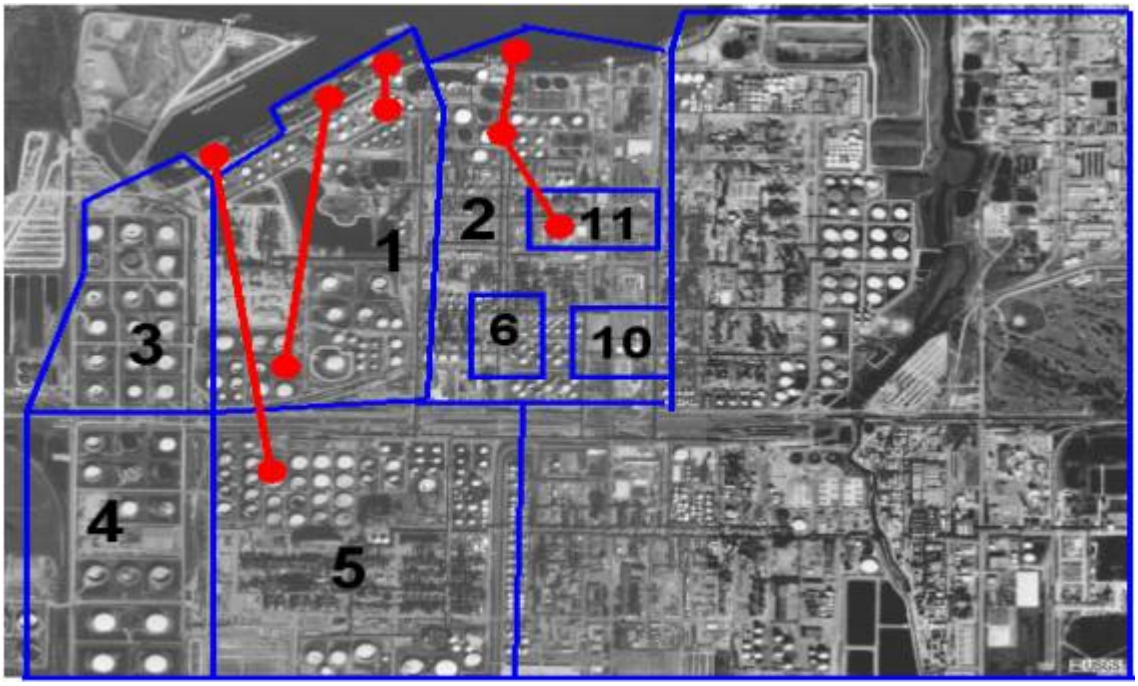
8.1.3. The COTP determines if a facility is isolated as defined in 33 CFR 105.105(c)(5). When making such a determination, the COTP should ensure that there is a lack of road access to the facility and that the facility does not distribute through secondary marine transfers. The COTP may wish to account for these facilities in the Area Maritime Security Plan Assessment, but there is no requirement for the COTP to issue a letter of determination to these facilities. However, if the facility is isolated but does conduct secondary marine transfers, that facility's owner/operator must submit a request for a waiver in accordance with 33 CFR 105.130.

Regulatory Application Models

Image 1

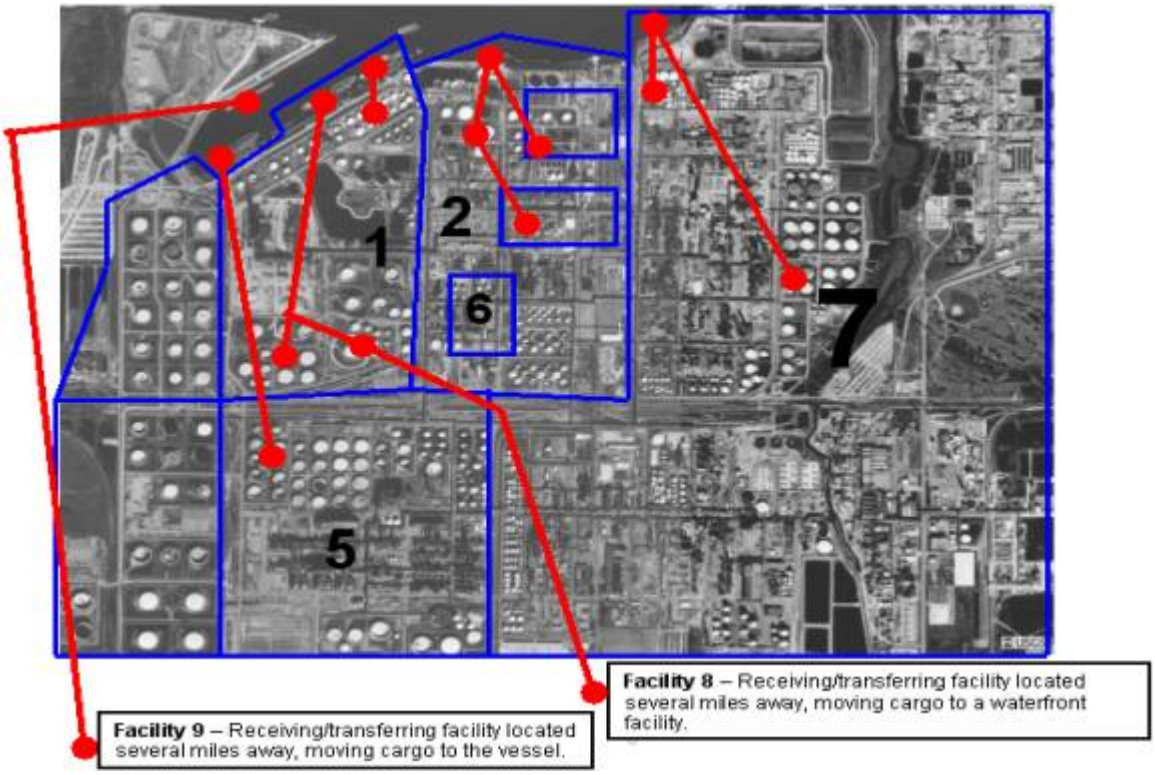
Scenario (Image 1)	**Description**	**Regulated Area**
1	A Marine Transportation Related (MTR) facility transferring cargo through a pipeline crosses a public street. However, the first valve within containment is located on the facility property across the street.	Both facility locations are regulated by 33 CFR 105. The facility's security assessment will highlight how the properties are inter-related.
2	A MTR facility transferring cargo through a pipeline crosses a public street. In this scenario the first valve within containment is located on the waterfront portion of the facility.	If there is access control for the facility where the valve within containment is located, then only that portion of the facility is regulated under 33 CFR 105. If there are any control systems outside the area described above, then the facility on which the controls are located will be regulated by 33 CFR 105.

Image 2



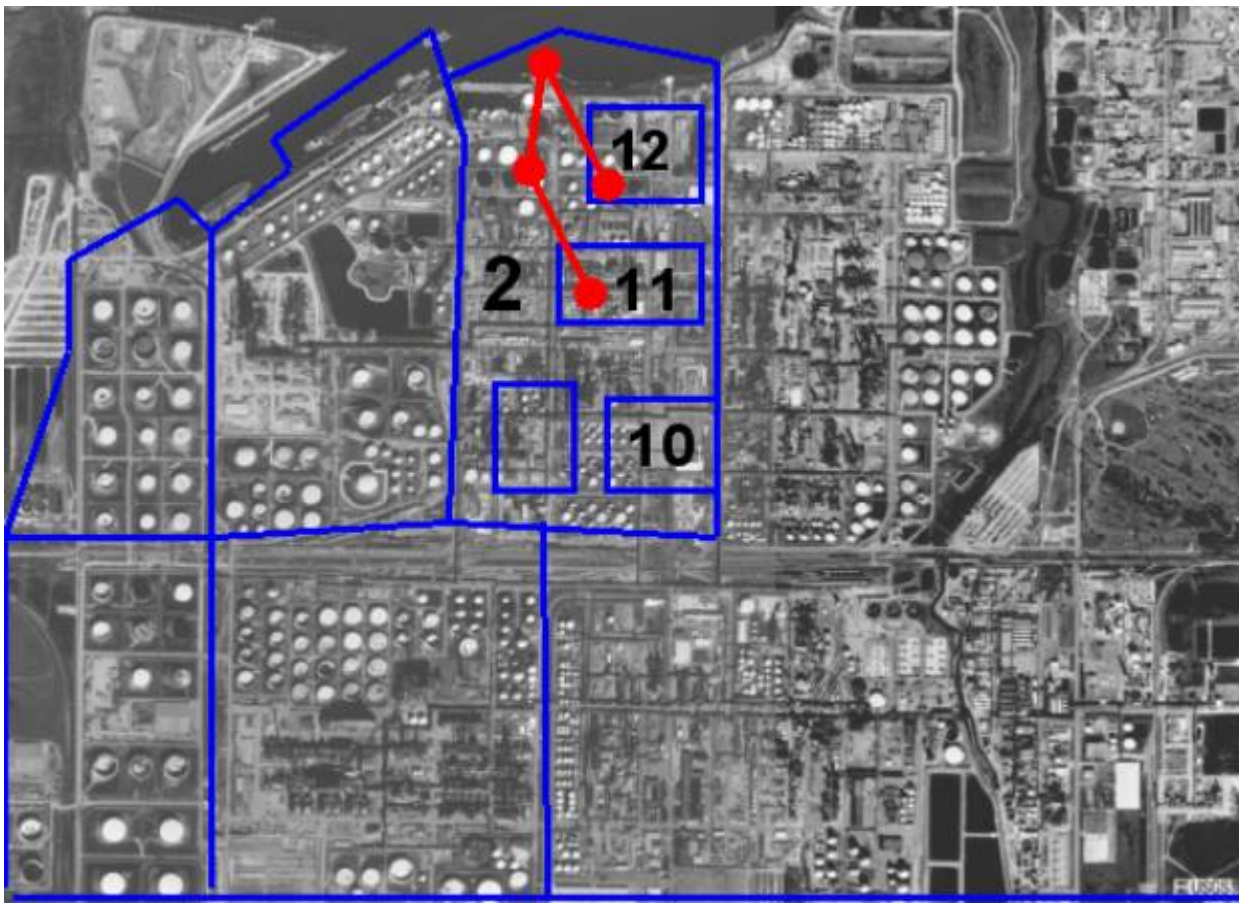
Scenario (Image 2)	**Description**	**Regulated Area**
3	**Facility 1** is located along the waterfront transferring cargo to storage tanks adjacent to the waterfront, and to tanks within the manufacturing facility not adjacent to the waterfront.	**Facility 1** is regulated by 33 CFR 105. The vulnerability assessment will identify any restricted areas within the facility or identify the entire facility as a restricted area.
4	**Facility 2** is located along the waterfront. In addition, there are multiple facilities owned/operated by other companies within Facility 2. Facility 6 is located within Facility 2 and has no marine activities. Facility 10 is located inside Facility 2 and along the perimeter, but has a separate entrance and exit. Facility 11 is located within Facility 2 and transfers cargo to storage tanks along the waterfront.	**Facility 2** is regulated by 33 CFR 105. Facility 2 would identify any restricted areas within the facility or designate the entire facility as a restricted area. The security plan of Facility 2 should address security measures for Facility 6, 10, and 11, which are enclosed within its perimeter (i.e., for access control, etc.) Facilities 6, 10, and 11 are not regulated by 33 CFR 105.
5	**Facility 3** is located on the waterfront, but has no Marine Transportation Related (MTR) activities.	**Facility 3** is not regulated by the Coast Guard, and, therefore, would not be subject to the 33 CFR 105 requirements.
6	**Facility 4** is located near the waterfront, but is not actually on the waterfront and does not have any MTR activities.	**Facility 4** is not regulated by the Coast Guard, and, therefore, would not be subject to the 33 CFR 105 requirements.

Image 3



Scenario (Image 3)	Description	Regulated Area
7	**Facility 5** is not located on the waterfront itself, but it does have a MTR facility, which transfers product back into the storage tanks within the facility. The "first valve within containment" is located near the tank farm area (not on the dock).	**Facility 5** is regulated and is required to be in compliance with 33 CFR 105. If the MTR facility has access control and is where the first valve within containment is located, **Facility 5** would not be subject to 33 CFR 105.
8	**Facility 6** is located inside Facility 2. Facility 6 does not have any MTR activities, and is not located on the waterfront. Facility 2 must be entered to gain access to Facility 6 (there is no external entrance to Facility 6).	**Facility 6** shall be accounted for in the Vulnerability Assessment and FSP of Facility 2. Facility 6 is not subject to 33 CFR 105.
9	**Facility 7** is similar to Facility 1 located along the waterfront, and transfers cargo to storage tanks adjacent to the waterway, and to tanks within the production facility not adjacent to the waterfront.	Facility 7 is required to be in compliance with 33 CFR 105. The plan will identify any restricted areas within the facility or consider the entire facility as a restricted area.
10	**Facility 8** is a separate company located several miles from the waterfront and transfers cargo to and from Facility 1,which transfers cargo to the MTR facility.	The transfer operation will be considered in the assessment for Facility 1. Facility 8 will not have to be in compliance with 33 CFR 105.
11	**Facility 9** transfers cargo through a pipeline from a MTR to a receiving/transferring facility located several miles away. The first valve within containment is located at the receiving/transferring facility several miles from the waterfront.	Facility 9 is regulated by 33 CFR 105. The plan will incorporate the marine facility, the pipeline, and the receiving facility.

Image 4



Scenario (Image 4)	**Description**	**Regulated Area**
12	**Facility 10** is located within Facility 2. However, Facility 10 has its own access control (Access through Facility 2 is not necessary to enter Facility 10.)	Facility 10 is not subject to 33 CFR 105.
13	**Facility 11** is located within Facility 2, and personnel must pass through access control of Facility 2 to enter Facility 11. Facility 11 transfers cargo to a storage tank located within Facility 2, which transfers cargo to/from vessels.	Facility 11 will to be considered as part of the assessment of Facility 2. Facility 11 is not required to be in compliance with 33 CFR 105.
14	**Facility 12** is located within Facility 2, and personnel must pass through access point for Facility 2 to enter Facility 12. Facility 12 transfers cargo to and from vessels.	Facility 12 is regulated under 33 CFR 105.

Image 5

Scenario (Image 5)	**Description**	**Regulated Area**
15	Facility in image 5 is a dock that has a casino boat permanently moored at a dock.	If the vessel is permanently moored and does not have a certificate of inspection, neither the vessel nor the facility will be regulated by 33 CFR 105.
16	A facility similar to the one in image 5 services cruise-type vessels that depart from facility, sail up and down the river, and then returns to the same facility to disembark the passengers.	Both the vessel and facility are required to have separate plans. They can have a combined plan, but will have to submit it to both the MSC and COTP, and will have to have an index to cross-reference the vessel and facility requirements.
17	(No image provided) A ferry embarks and disembarks passengers and vehicles at two separate facilities.	The vessel and the facilities are required to be in compliance with 33 CFR 104 and 105. The separate plans may be consolidated into one. The consolidated plan will have to be submitted to both MSC (for vessels) and the local COTP (for the facilities). The consolidated plan will be cross-index for both vessels and facilities. The above situation refers to ferries that are not involved in coastwise or international voyages.
18	(No image provided) Facility receives a vessel on an ***international voyage*** carrying a non-hazardous material (i.e., rock, limestone, wood, timber, etc.) that calls on a manned/unmanned facility. In many cases, the vessel conducts the transfer operation with no shore assistance.	If the vessel exceeds 100 GRT, the facility must be in compliance with 33 CFR 105 and develop a facility security plan.
19	(No image provided) The same as scenario 18 but the vessel is only on a domestic voyage.	Same as scenario 18 except the facility is not required to be in compliance with 33 CFR 105 if it only receives domestic route vessels less than 100 GRT and does not receive certain dangerous cargoes (CDCs).

ENCLOSURE 9
SAMPLE DECLARATION OF SECURITY (DoS)

Declaration of Security (DoS)
(Sample)

_____ (Name of Vessel)	_____ (Name of Facility)
_____ (IMO or VIN Number)	_____ (Location)
_____/_____ (Registry)/(Flag)	_____ (COTP Zone)

The affixing of initials below indicate that the activity will be done, in accordance with the relevant approved security plan:

(Responsible party to initial space provided in columns)

Activity	**Vessel**	**Facility**
1. Communications established between the vessel and vessel/facility:	_____	_____
(a) Means of raising alarm agreed between vessel and vessel/facility.	_____	_____
(b) Vessel and facility communicates any noted security non-conformities and notify appropriate government agencies.	_____	_____
(c) Procedures established to notify local and federal authorities	_____	_____
2. Responsibility for checking identification and screening of:		
(a) Passengers, crew, hand carried items, and unaccompanied baggage.	_____	_____
(b) Vessel stores, cargo, and vehicles.	_____	_____
3. Responsibility for searching the berth/pier directly surrounding the vessel.	_____	_____
4. Responsibility for monitoring and/or performing security of water surrounding the vessel.	_____	_____
5. Responsibility for monitoring restricted areas.	_____	_____
6. Responsibility for controlling access to the port facility.	_____	_____
7. Responsibility for controlling access to the ship.	_____	_____
8. Ensuring the performance of all security duties.	_____	_____
9. Verification of increased MARSEC level and implementation of additional protective measures.	_____	_____

The signatories to this agreement certify that security arrangements meet the provisions of the Maritime Transportation Security Act of 2002.

Date of issue ……

_____ (Signature of *Master or Vessel Security Officer*)	_____ (Signature of *Facility Security Officer* or *authorized designee*)
_____ Printed Name and Title of *Master* or *Vessel Security Officer*	_____ Printed Name and Title of *Facility Security Officer* or *authorized designee*
Contact information_____	Contact information_____
_____	_____

ENCLOSURE 10
MTSA FACILITY COMPLIANCE GUIDE

Use of the MTSA Facility Compliance Guide

This guide is designed to assist Coast Guard Inspectors in conducting field compliance inspections of facility security plans (FSP) belonging to domestic U.S. facilities engaged in the transportation of cargo and passengers by water. This guide is composed of a compliance checklist to assist the inspector in ensuring key components of the MTSA regulations are verified.

There are four key steps that the Coast Guard inspector must follow in conducting a compliance inspection:

- **Ensure** the facility complies with the Facility Security Plan (FSP).
- **Ensure** the approved FSP/ASP adequately addresses the performance-based criteria as outlined in 33 CFR 105.
- **Ensure** the adequacy of the Facility Security Assessment (FSA) and the Facility Vulnerability and Security Measures Summary (CG-6025).
- **Ensure** that the measures in place adequately address the vulnerabilities.

MTSA regulations do not mandate specific equipment or procedures, but call for performance based criteria to ensure the security of the facility. While this guide is designed to assist the Coast Guard facility inspector, this guide cannot be used alone to verify the facility has adequate security measures. The review of the FSP and FVA requires interaction with the facility owner, operator, designated security officers and all personnel with related duties aboard the facility.

MTSA places the responsibility to complete an accurate security assessment, and to address the vulnerabilities in the Facility Security Plan (FSP), on the owner or operator of the facility. The Coast Guard has the responsibility to verify that the facility is complying with its approved plan.

Pre-inspection Items	Inspection Items	Post-inspection Items
• Review MISLE records • Review deficiency history • CG Activity History • Schedule inspection with FSO • Provide FSO with MTSA Facility Compliance Guide (enclosure 10 of NVIC 03-03) with instructions for FSO to complete prior to CG inspection	• Review FSP • Review FSA • Review CG-6025 • Review and complete the MTSA Facility Compliance Guide with assistance of facility FSO	• Complete MISLE *MTSA Compliance Exam* activity case • Determine whether amendments to the FSP are required • Initiate appropriate actions to ensure timely correction of deficiencies

Examinations shall address all areas of the MTSA regulations, and shall be done through observation of the current security procedures in place for each MARSEC Level; questioning facility personnel regarding security duties and procedures; verifying on site presence and validity of required security documents and certificates; as well as proper operation of security equipment. **This booklet is intended only as a guide to general MTSA requirements. Specific requirements will be contained in the Facility Security Plan (FSP).**

United States Coast Guard

MTSA FACILITY COMPLAINCE GUIDE

Name of Facility/Location	**Facility Type**
Facility ID Number	**MISLE Activity Number**
Date(s) Conducted	
Facility Inspectors 1. _____ 5. _____ 2. _____ 6. _____ 3. _____ 7. _____ 4. _____ 8. _____	

Guidance for completing the MTSA Facility Compliance Guide (checklist) –
Coast Guard facility inspectors and facility security officers (FSOs) shall complete the checklist by addressing each item contained therein. Completion of the check boxes is mandatory for all items. Each item contained in the guide (checklist) must be notated as one of the following:

Sat – Item satisfactorily meets requirements contained in the guide and referenced regulations.
N/O – Item was Not Observed during this inspection.
N/A - Item is Not Applicable to this facility or inspection.
Fail - Item was found to be unsatisfactory and therefore failed inspection.

Compliance documentation *33 CFR 105.120*	SAT	N/O	N/A	FAIL
1. Approved **Facility Security Plan (FSP) or**				
1.1. Review the FSP	☐	☐	☐	☐
1.2. Review the Facility Security Assessment and CG-6025	☐	☐	☐	☐
2. **Letter of Authorization to Operate (LOA) or**				
2.1. Review the submitted FSP	☐	☐	☐	☐
2.2. Review the submitted Facility Security Assessment and CG-6025	☐	☐	☐	☐
3. **Alternative Security Program**, with letter signed by facility owner/operator				
3.1. Review ASP	☐	☐	☐	☐
3.2. Review the Facility Security Assessment and CG-6025	☐	☐	☐	☐

Non-Compliance *33 CFR 105.125*	SAT	N/O	N/A	FAIL
4. Conditions existing (if any):				
4.1. 1) _____	☐	☐	☐	☐
4.2. 2) _____	☐	☐	☐	☐
5. Conditions met.	☐	☐	☐	☐
6. COTP notified of non-compliance?	☐	☐	☐	☐

Waivers & Equivalents *33 CFR 105.130 & 105.135*	SAT	N/O	N/A	FAIL
7. Approval letter for waiver from Commandant G-MP.	☐	☐	☐	☐
8. Approval letter for equivalent from Commandant G-MP.	☐	☐	☐	☐

Maritime Security (MARSEC) Directives *33 CFR 105.145*	SAT	N/O	N/A	FAIL
9. Incorporated in to security plan.	☐	☐	☐	☐

Facility Security Officer Knowledge & Training *33 CFR 105.205*	SAT	N/O	N/A	FAIL
10. Name of FSO: _____				
11. FSO Contact Information:				
11.1. Primary phone number **( )** _____ - _____				
11.2. Secondary number **( )** _____ - _____				
12. Is FSO familiar with FSP and relevant portions of the regulations? FSO must have general knowledge through training or equivalent job experience in the following:				
12.1. Facility security organization	☐	☐	☐	☐
12.2. Vessel and facility security measures to be implemented at the different MARSEC Levels	☐	☐	☐	☐
12.3. Familiarity with security equipment and systems, and their operational limitations	☐	☐	☐	☐
12.4. Familiarity with methods of conducting audits, inspections, control, and monitoring techniques	☐	☐	☐	☐
FSO must have knowledge and receive training in the following, as appropriate:				
12.5. Risk assessment methodology	☐	☐	☐	☐
12.6. Methods of facility security surveys and inspections	☐	☐	☐	☐
12.7. Instruction techniques for security training and education, including security measures and procedures	☐	☐	☐	☐
12.8. Handling (as well as access to and distribution of) sensitive security information and security related communications	☐	☐	☐	☐
12.9. Current security threats and patterns	☐	☐	☐	☐
12.10. Recognizing and detecting dangerous substances and devices	☐	☐	☐	☐
12.11. Recognizing characteristics and behavioral patterns of persons who are likely to threaten security	☐	☐	☐	☐
12.12. Techniques used to circumvent security measures	☐	☐	☐	☐
12.13. Conducting physical searches and non-intrusive inspections	☐	☐	☐	☐
12.14. Conducting security drills and exercises, including exercises with vessels	☐	☐	☐	☐
12.15. Assessing security drills and exercises	☐	☐	☐	☐

Facility Personnel With Security Duties ***33 CFR 105.210***	SAT	N/O	N/A	FAIL
13. **Verify** that personnel **with security duties** are familiar with FSP and relevant portions of the regulations? These personnel must have general knowledge through training or equivalent job experience in the following:				
13.1. Current security threats and patterns	☐	☐	☐	☐
13.2. Testing, calibration, operation, and maintenance of security equipment and systems	☐	☐	☐	☐
13.3. Security related communications (including the handling of SSI)	☐	☐	☐	☐
13.4. Methods of physical screening of persons	☐	☐	☐	☐
13.5. Knowledge of emergency procedures and contingency plans	☐	☐	☐	☐
13.6. Techniques used to circumvent security systems	☐	☐	☐	☐
13.7. Recognition of characteristics and behavioral patterns of persons who are likely to threaten security	☐	☐	☐	☐
13.8. Recognition and detection of dangerous substances and devices	☐	☐	☐	☐
13.9. Inspection, control, and monitoring techniques.	☐	☐	☐	☐
13.10. The meaning and the consequential requirements of the different MARSEC levels	☐	☐	☐	☐

Facility Personnel Without Security Duties ***33 CFR 105.210 & 105.215***	SAT	N/O	N/A	FAIL
14. **Verify** that all other personnel are familiar with FSP and relevant portions of the regulations. These personnel must have general knowledge through training or equivalent job experience in the following:				
14.1. Relevant provisions of the FSP & meaning of different MARSEC levels.	☐	☐	☐	☐
14.2. Recognition & detection of dangerous substances and devices.	☐	☐	☐	☐
14.3. Recognition of characteristics and behavioral patterns of persons who are likely to threaten security.	☐	☐	☐	☐
14.4. Techniques used to circumvent security measures.	☐	☐	☐	☐

Drill & Exercise Requirements *33 CFR 105.220*	SAT	N/O	N/A	FAIL
15. **Review** Drill Log to ensure drills are conducted at least every 3 months.	☐	☐	☐	☐
15.1. Date/Type of Last Drill: _____				
16. **Review** Exercise Log to ensure exercises are conducted each calendar year, no more than 18 months between exercises.	☐	☐	☐	☐
16.1 Date/Type of Last Exercise: _____				

Facility record keeping requirements *33 CFR 105.225*	SAT	N/O	N/A	FAIL
17. **Review** records to ensure all of the following are recorded -				
17.1. Breaches of security	☐	☐	☐	☐
17.2. Changes in Maritime Security (MARSEC) Levels	☐	☐	☐	☐
17.3. Maintenance, calibration, and testing of security equipment	☐	☐	☐	☐
17.4. Security threats	☐	☐	☐	☐
17.5. Training records for facility personnel with **security duties ONLY.** (*Those personnel covered under 33 CFR 105.210*)				
17.5.1 Date of each training session	☐	☐	☐	☐
17.5.2. Duration	☐	☐	☐	☐
17.5.3. Description of training	☐	☐	☐	☐
17.5.4. List of attendees	☐	☐	☐	☐
17.6. **Verify** that all records are maintained for at least (2) years.	☐	☐	☐	☐
17.7. **Verify** that the FSP/ASP undergoes an annual audit.				
17.7.1. Check the document(s) signed by FSO certifying the annual audit.	☐	☐	☐	☐
17.7.2. Verify that past audit findings are addressed.	☐	☐	☐	☐
18. **Verify** the FSP is being protected from unauthorized disclosure in accordance with SSI procedures.	☐	☐	☐	☐

MARSEC Level Coordination & Implementation ***33 CFR 105.230***	SAT	N/O	N/A	FAIL
19. **Ensure** facility is operating at proper MARSEC level in effect for the Port.				
19.1. **Review procedures** outlined in FSP for current MARSEC level	☐	☐	☐	☐
20. **Review** the procedures for changes in MARSEC levels.				
20.1. MARSEC Level I to 2	☐	☐	☐	☐
20.2. MARSEC Level 2 to 3	☐	☐	☐	☐
21. 12 Hour implementation timeframe & reporting to COTP.	☐	☐	☐	☐

Communications ***33 CFR 105.235***	SAT	N/O	N/A	FAIL
22. **Verify** that primary and backup communications **systems** and **procedures** allow effective and continuous communications between the facility security personnel, vessels interfacing w/facility, the COTP and authorities w/security responsibilities.	☐	☐	☐	☐
23. **Verify** that each active facility access point provides a means of contacting police, security control, or an emergency operations center.	☐	☐	☐	☐

Declaration of Security ***33 CFR 105.225 & 105.245***	SAT	N/O	N/A	FAIL
24. **Verify** that DoS's are maintained for 90 days.	☐	☐	☐	☐
25. When a continuing DoS is used, the FSP/ASP must **ensure** that:				
25.1. The DoS is valid for a specific MARSEC Level.	☐	☐	☐	☐
25.2. The effective period at MARSEC Level 1 does not exceed 90 days.	☐	☐	☐	☐
25.3. The effective period at MARSEC Level 2 does not exceed 30 days.	☐	☐	☐	☐

Security systems and equipment maintenance ***33 CFR 105.250***	SAT	N/O	N/A	FAIL
26. **Verify** security systems and equipment are in good working order and inspected, tested, calibrated, and maintained according to Manufacturers' recommendations.	☐	☐	☐	☐
27. **Verify** procedures for identifying and responding to security and equipment failures or malfunctions.	☐	☐	☐	☐

Security measures for access control ***33 CFR 105.255***	SAT	N/O	N/A	FAIL
28. **VERIFY** procedures at **MARSEC Level 1** to ensure that security measures relating to access control are implemented **AS OUTLINED IN THE FSP**, these procedures include those that:				
28.1. Screen persons, baggage, personal effects, and vehicles, for dangerous substances and devices at the rate specified in the approved FSP.	☐	☐	☐	☐
28.2. Conspicuously post signs that describe security measures currently in effect and clearly state the entering the facility is deemed valid consent to screening or inspection, and that failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter.	☐	☐	☐	☐
28.3. Check the identification of any person seeking to enter the facility, including vessel passengers and crew, facility employees, vendors, visitors.	☐	☐	☐	☐
28.4. Identify access points that must be secured or attended to deter unauthorized access.	☐	☐	☐	☐
28.5. Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel.	☐	☐	☐	☐
28.6. Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between facility and vessel.	☐	☐	☐	☐
29. **REVIEW** procedures for **MARSEC Level 2** to ensure that security measures relating to access control can be implemented **AS OUTLINED IN THE FSP**.	☐	☐	☐	☐
30. **REVEIW** procedures for **MARSEC Level 3** to ensure that security measures relating to access control can be implemented **AS OUTLINED IN THE FSP**.	☐	☐	☐	☐

Security measures for restricted areas ***33 CFR 105.260***	SAT	N/O	N/A	FAIL
31. **VERIFY** procedures to ensure that security measures relating to restricted area access control are implemented **AS OUTLINED IN THE FSP**. These procedures include those that:				
31.1. Identify which facility members are authorized access.	☐	☐	☐	☐
31.2. Identify when other personnel are authorized access.	☐	☐	☐	☐
31.3. Define the extent of any restricted area.	☐	☐	☐	☐
31.4. Define the times when access restrictions apply.	☐	☐	☐	☐
- Section continued on next page -				

Security measures for restricted areas *33 CFR 105.260*	SAT	N/O	N/A	FAIL
31.5. Clearly mark all restricted areas.	☐	☐	☐	☐
31.6. Control entry, parking, loading and unloading of vehicles.	☐	☐	☐	☐
31.7. Control the movement and storage of cargo and vessel stores.	☐	☐	☐	☐
31.8. Control unaccompanied baggage or personnel effects.	☐	☐	☐	☐
32. **VERIFY** procedures at **MARSEC Level 1** to ensure that security measures relating to restricted areas are implemented **AS OUTLINED IN THE FSP**.	☐	☐	☐	☐
33. **REVIEW** procedures for **MARSEC Level 2** to ensure that security measures relating to restricted areas can be implemented **AS OUTLINED IN THE FSP**.	☐	☐	☐	☐
34. **REVIEW** procedures for **MARSEC Level 3** to ensure that security measures relating to restricted areas can be implemented **AS OUTLINED IN THE FSP**.	☐	☐	☐	☐

Security measures for handling cargo *33 CFR 105.265*	SAT	N/O	N/A	FAIL
35. **VERIFY** procedures at **MARSEC Level 1** to ensure that security measures relating to handling cargo are implemented **AS OUTLINED IN THE FSP**. These procedures include those that:				
35.1. Routinely check cargo, cargo transport units, and cargo storage areas within the facility prior to, and during, cargo handling ops to deter tampering.	☐	☐	☐	☐
35.2. Check that cargo, containers, or other cargo transport units entering the facility match the delivery note or equivalent cargo documentation.	☐	☐	☐	☐
35.3. Screen vehicles.	☐	☐	☐	☐
35.4. Check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility.	☐	☐	☐	☐
36. **REVIEW** procedures for **MARSEC Level 2** to ensure that security measures relating to handling of cargo can be implemented **AS OUTLINED IN THE FSP**.	☐	☐	☐	☐
37. **REVIEW** procedures for **MARSEC Level 3** to ensure that security measures relating to handling of cargo can be implemented **AS OUTLINED IN THE FSP**.	☐	☐	☐	☐

Security measures for delivery of vessel stores and bunkers ***33 CFR 105.270***	SAT	N/O	N/A	FAIL
38. **VERIFY** procedures at **MARSEC Level 1** to ensure that security measures relating to delivery of vessel stores and bunkers are implemented **AS OUTLINED IN THE FSP**, these procedures must include those that:				
38.1. Screen stores at rate specified in FSP.	☐	☐	☐	☐
38.2. Require advance notice of deliveries.	☐	☐	☐	☐
38.3. Screening delivery vehicles at rate specified in FSP.	☐	☐	☐	☐
39. **REVIEW** procedures for **MARSEC Level 2** to ensure that security measures relating to delivery of vessel stores and bunkers can be implemented **AS OUTLINED IN THE FSP**.	☐	☐	☐	☐
40. **REVIEW** procedures for **MARSEC Level 3** to ensure that security measures relating to delivery of vessel stores and bunkers can be implemented **AS OUTLINED IN THE FSP**.	☐	☐	☐	☐

Security measures for monitoring ***33 CFR 105.275***	SAT	N/O	N/A	FAIL
41. **VERIFY** procedures at **MARSEC Level 1** to ensure that security measures relating to monitoring are implemented **AS OUTLINED IN THE FSP**. These procedures include those that:				
41.1. Monitor the facility area, including shore and waterside access.	☐	☐	☐	☐
41.2. Are capable to monitoring access points, barriers and restricted areas.	☐	☐	☐	☐
41.3. Are capable of monitoring access and movement adjacent to vessels using the facility, including augmentation of lighting utilized by vessels.	☐	☐	☐	☐
42. **REVIEW** procedures for **MARSEC Level 2** to ensure that security measures relating to monitoring can be implemented **AS OUTLINED IN THE FSP.**	☐	☐	☐	☐
43. **REVIEW** procedures for **MARSEC Level 3** to ensure that security measures relating to monitoring can be implemented **AS OUTLINED IN THE FSP.**	☐	☐	☐	☐

Security incident procedures ***33 CFR 105.280***	SAT	N/O	N/A	FAIL
44. **Verify** procedures for responding to security threats or breaches of security and maintaining critical facility and vessel-to-facility interface.	☐	☐	☐	☐
45. **Review** procedures for reporting security incidents.	☐	☐	☐	☐

Passenger and Ferry Facilities Only ***33 CFR 105.285***	SAT	N/O	N/A	FAIL
46. **Verify** areas are established to segregate unchecked persons and effects from checked persons and effects.	☐	☐	☐	☐
47. **Verify** vehicles are being screened IAW the FSP/ASP.	☐	☐	☐	☐
48. **Verify** security personnel control access to restricted areas.	☐	☐	☐	☐
49. **Verify** sufficient security personnel to monitor all persons within the area.	☐	☐	☐	☐

Cruise Ship Terminals Only ***33 CFR 105.290***	SAT	N/O	N/A	FAIL
50. **Verify** procedures to screen all persons, baggage, and all personal effects for dangerous substances and devices.	☐	☐	☐	☐
51. **Verify** procedures for checking personnel identification.	☐	☐	☐	☐
52. **Inspect** designated holding, waiting, or embarkation areas to segregate screened persons and their effects.	☐	☐	☐	☐
53. **Verify** procedures to provide additional security personnel to designated holding areas and deny passengers access to the restricted areas.	☐	☐	☐	☐

Certain Dangerous Cargo (CDC) Facilities Only ***33 CFR 105.295***	SAT	N/O	N/A	FAIL
54. **Verify** procedures to escort all visitors, contractors, vendors, and other non-facility employees.	☐	☐	☐	☐
55. **Verify** procedures for controlling parking, loading and unloading of vehicles.	☐	☐	☐	☐
56. **Verify** procedures for security personnel to record or report their presence at key points during security patrols.	☐	☐	☐	☐
57. **Verify** procedures to search key areas prior to vessel arrivals.	☐	☐	☐	☐
58. **Inspect** alternate or independent power source.	☐	☐	☐	☐

Barge Fleeting Facilities Only ***33 CFR 105.296***	SAT	N/O	N/A	FAIL
59. **Verify** designated restricted areas within the barge fleeting facility.	☐	☐	☐	☐
60. **Inspect** current list of vessels and cargoes in the designated restricted area.	☐	☐	☐	☐
61. **Verify** that there is at least one tug available to service the facility for every 100 barges.	☐	☐	☐	☐
**Barge Fleeting Facilities are exempt from Security Measures for Handling Cargo and Security measures for delivery of vessel stores and bunkers*.				

--- Notes on deficiencies ---

Two distinct types of deficiencies may be identified utilizing this compliance checklist -

Facility is not operating in accordance with their approved/submitted FSP or ASP – This type of deficiency is addressed utilizing a range of enforcement and compliance measures, from Lesser Administrative actions (worklists, etc.), up to and including more significant measures such as Notice of Violations, Civil Penalties, and Operational Controls which may restrict facility operations.

Facility is operating in accordance with their approved/submitted FSP or ASP, but plan does not meet the specific performance criteria outlined in the regulations – These types of deficiencies must be addressed through the plan amendment guidance as set forth in 33 CFR 105.415 (*excerpt provided below*).

> "(a) Amendments to a Facility Security Plan (FSP) that is approved by the cognizant COTP may be initiated by" "(ii) the cognizant COTP upon a determination that an amendment is needed to maintain the facility's security. The cognizant COTP will give the facility owner or operator written notice and request that the facility owner or operator propose amendments addressing any matters specified in the notice. The facility owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the COTP".

Generally, items in the checklist beginning with "*Verify procedures*" indicate issues requiring plan amendments. These sections include, but are not limited to:

Communications, *22 – 23*
Security measures for access control, *28*
Security measures for restricted areas, *31*
Security measures for handling cargo, *35*
Security measures for delivery of vessel stores and bunkers, *38*
Security measures for monitoring, *41*
Security incident procedures, *44 – 45*
Passenger and Ferry facilities only, *46*
Cruise Ship Terminals only, *50 – 51, 53*
CDC facilities only, *54 – 57*
Barge fleeting facilities only, *59*

--- Inspection Summary included on next page ---

Inspection Summary

Comments:

ENCLOSURE 11
ADDITIONAL POLICY GUIDANCE

11.1. Enclosure Contents

11.1.1. This enclosure contains the following additional policy guidance:

11.2 Introduction

11.2.1. Regulations mandated by the Maritime Transportation Security Act of 2002 (MTSA) and the International Ship and Port Facility Security (ISPS) Code place the responsibility of completing an accurate security assessment and addressing the vulnerabilities identified in the Facility Security Plan (FSP) on the owner or operator of a facility. The Coast Guard has the responsibility to review and approve the FSP and verify that the facility is complying with an approved FSP. This enclosure is provided to supplement existing guidance outlined in NVIC 03-03 (predominately enclosure (2), MTSA FSP/ASP Implementation Process Methodology), the preambles to the Interim Rule and the Final Rule, and other policy guidance promulgated by the Coast Guard.

11.2.2. Additional guidance concerning the issuance of approval letters and letters of authorization, discussed in sections 11.7 thru 11.9, is contained in Addendum (1) to this enclosure. This flowchart is provided as a decision-tool to assist the COTP in determining the proper course(s) of action during the FSP review and approval stage.

11.2.3. As additional guidance continues to be developed, the MTSA-ISPS Helpdesk website at http://www.uscg.mil/hq/g-m/mp/MTSA.shtml should be consulted regularly for the most current policy guidance and information.

11.3 Plan Submission

11.3.1. On July 1, 2004, any facility that was operating prior to December 31, 2003, or that entered service prior to June 30, 2004, and was in a service subject to the requirements of MTSA, that does not submit an FSP or a letter stating which Alternative Security Program (ASP) will be used will not be allowed to continue to operate in such a service. Any facility that does operate in a MTSA related service without a submitted FSP or ASP will be issued a Captain of the Port (COTP) order directing the facility to cease MTSA related operations. Appropriate civil penalty action will also be initiated against the facility owner, operator, or both.

11.3.2. New facilities (those entering service on or after July 1, 2004) must submit their FSP 60 days prior to beginning MTSA related operations.

11.4. Compliance documentation

11.4.1. On July 1, 2004, each facility subject to MTSA must have documentation supporting one of the following:

- Accepted ASP
- Approved FSP
- Interim Approved FSP
- Letter of Authorization (LOA) permitting a facility to continue operations provided the facility remains in compliance with the submitted FSP.

11.5 Alternative Security Programs (ASP)

11.5.1. Commandant (G-MP) is responsible for approving Alternative Security Programs (ASPs). Once approved, owners or operators of facilities may use an ASP if it is appropriate for that facility. Owners or operators must submit a letter to the cognizant Captain of the Port (COTP) stating which approved ASP the owner or operator will use. The National Facility Security Plan Review Center (NFSPRC) accepts and reviews letters submitted by owners or operators who are intending to implement an approved ASP.

11.5.2. The procedures for accepting ASPs are contained in enclosure (2), section 2.8. In accordance with this guidance, ASPs do not undergo the same "staged" process that applies to FSPs. As such, facilities that utilize ASPs are not subject to a Stage III review by the COTP. After 30 June 2004, these facilities are subject to the same inspection requirements as those utilizing FSPs. See section 11.11 of this enclosure for further discussion of inspection policies**.**

11.6 Temporary equivalent security measures

11.6.1. A facility that is not capable of implementing substantial aspects of their approved (or submitted) facility security plan on 1 July 2004 will be required to identify and implement equivalent but temporary

security measures when the installation of physical security equipment is pending. The temporary equivalent security measures should be identified in writing and submitted to the cognizant Captain of the Port. The following elements of the facility security plan, when substantially deficient, will normally be subject to temporary equivalent security measures:

- FSO training/qualifications;
- Effective means of communication;
- Security measures for access control;
- Security measures for restricted areas;
- Security measures for handling cargo;
- Security measures for delivery of vessel stores/bunkers;
- Security measures for monitoring; or
- Procedures for completing a DoS and performing the facility/vessel interface

11.6.2. Prior to approving any temporary equivalent security measures, COTPs should perform an evaluation to determine that the proposed measures are equivalent and that they fulfill the intent of the approved security measures within the FSP. COTPs are authorized to approve these measures for periods not to exceed four (4) months, District Commanders are authorized to approve measures for periods not to exceed eight (8) months, and Area Commanders are authorized to approve measures for periods not to exceed twelve (12) months. COTPs, District and Area Commanders, and their staffs, using experience and good judgment, will evaluate these temporary equivalent security measures, taking into account the following guidance:

- Can the proposed measures be implemented on 1 July 2004?
- Do the proposed measures serve the purpose of the measures they are being substituted for?
- Do the proposed measures provide sufficient time for the facility to implement the measures identified in the FSP?
- Do the proposed measures provide estimated completion dates and provide sufficient supporting documentation to confirm the approved measures are being procured (as applicable e.g. equipment, fencing, etc.)?
- Are the proposed measures consistent with guidance issued by Area and District Commanders, as applicable?

11.6.3. The following scenario provides an example in determining temporary equivalent security measures: A facility reports that the surveillance camera it has identified in its approved plan cannot be installed until August 2004. The facility proposes to use a roving security guard until the surveillance camera is installed. The application states that the facility has contracted with a guard service to provide a guard who will make hourly rounds of the facility and will be equipped with appropriate communications equipment. The application further states the camera is on order and contains a receipt or contract from the provider that the camera is expected to be installed no later than 30 August 2004. Unless the size of the facility is an issue or the risk of the facility is unusually high, this proposal could be considered an acceptable temporary equivalent security measure.

11.6.4. COTPs should ensure the cognizant District Commanders are informed of all decisions made with regards to temporary equivalent security measures. District Commanders should review all decisions for consistency throughout their areas of responsibility.

11.7 FSP Letter of Approval

11.7.1. The NFSPRC is performing Stage I and Stage II review of all FSPs. When the Stage II review is complete, the NSFPRC will deliver the FSP to the COTP for Stage III review and approval.

11.7.2. The COTP will perform the Stage III review before approving the FSP. The Stage III FSP review consists of reviewing Stage II carry-over items and validating the vulnerability assessment. This review does not require a comprehensive review of the FSP and may not require a site visit. The COTP will use the Stage III checklist located in enclosure (6) when completing the approval process. Although conducting a facility visit is recommended to validate applicability of the FSP at the site, the COTP may determine a site visit is optional based on familiarity with the facility, the facility's inspection history, and the risk the facility presents. In accordance with enclosure (6), the purpose of conducting a site visit during Stage III review is to validate applicability of the FSP at the facility and not to ensure facility compliance with the FSP. Verification of compliance will be conducted after 30 June 2004, in accordance with 11.12 of this enclosure and 2.10 of enclosure (2).

11.7.3. Prior to June 30, 2004, the FSP does not need to be fully implemented for the Stage III review to be conducted or the FSP to be approved. If the Stage III review is satisfactory, the COTP should issue a FSP letter of approval. A sample FSP letter of approval is included in enclosure (7).

11.7.4. Facilities that receive a letter of approval may be required to implement temporary equivalent security measures when they cannot implement substantial aspects of their approved facility security plan on 1 July 2004. Guidance for addressing these temporary equivalent security measures is contained in Section 11.6 of this enclosure.

11.7.5. For all FSP review activity after the FSP is received by the COTP from NFSPRC, COTPs must ensure appropriate Marine Information Safety/Law Enforcement (MISLE) database entries are performed in accordance with the Documentation of Maritime Security Activities for Domestic Facilities (MTSA) User Guide located at http://mislenet.osc.uscg.mil/user_guides.aspx.

11.8 Interim Letter of Approval (ILA)

11.8.1. Effective June 1, 2004, the COTP may issue an Interim Letter of Approval (ILA) to facilities that have passed Stage I of the review process. A facility will generally be eligible to receive an ILA provided plan deficiencies are administrative in nature (see items B1-B6 of Addendum 1). ILAs will be issued with an expiration date of October 31, 2004. A sample ILA is included in enclosure (7).

11.8.2. Prior to issuing the ILA, the COTP may review the current Stage II plan review deficiency letter provided by the NFSPRC. If the FSP is otherwise complete but requires additional administrative changes, the COTP may issue an ILA to the facility. Changes to the plan will continue to be coordinated through the NFSPRC.

11.8.3. Facilities that receive an ILA may be required to implement temporary equivalent security measures when they cannot implement substantial aspects of their facility security plan on 1 July 2004. Guidance for addressing these temporary equivalent security measures is contained in Section 11.6 of this enclosure. These temporary equivalent security measures may not be related to the administrative deficiencies in paragraph 8.2.2.

11.8.4. When deciding whether the deficiencies are administrative in nature, the COTP may consult the NFSPRC. The COTP may also consult the facility owner or operator when making this determination.

11.9 Letter of Authorization (LOA)

11.9.1. Effective June 1, 2004, the COTP may issue a Letter of Authorization (LOA) to a facility to operate from July 1, 2004, until October 31, 2004. Facility owner or operators that submitted a FSP, passed Stage I of the FSP review process, met any plan correction deadlines but still require substantial revisions to their FSP, will generally be eligible to receive a LOA. After consulting the Stage II deficiency letter provided by the NFSPRC, the COTP should identify those areas of the FSP that require substantial revisions. The facility owner/operator should then develop temporary equivalent security measures to the satisfaction of the COTP. The following elements of the facility security plan, when substantially deficient, will normally be subject to temporary equivalent security measures:

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

11.9.2. Facilities that have responded to the NFSPRC with FSP amendments that appear to satisfactorily address all substantive issues raised in the current Stage II plan review letter should be considered for an Interim Letter of Approval. Facilities that have not yet received a Stage II plan approval or a Stage II plan review deficiency letter or addressed all substantial deficiencies raised in the Stage II review should be considered for a Letter of Authorization. The COTP may also consult the NFSPRC and/or the owner or operator when making this determination.

11.9.3. Facilities that receive a Letter of Authorization will be required to implement temporary equivalent security measures for the substantial deficiencies discussed in 11.9.2. Guidance for addressing these temporary equivalent security measures is contained in Section 11.6 of this enclosure.

11.10 Non-Compliant Facilities

11.10.1. Facilities will be considered "non-compliant" for the purposes of 33 CFR 105 and will not be authorized to conduct any MTSA related operations beginning July 1, 2004, if they are ineligible to receive a FSP letter of approval, ILA, or LOA, and they are not operating under an approved ASP.

11.10.2. A facility owner/operator that receives a LOA but does not implement temporary equivalent security measures to the satisfaction of the COTP will have the LOA revoked and will not be authorized to conduct any MTSA related operations.

11.10.3. COTPs will identify all non-compliant facilities in their area of responsibility and engage the owners or operators of these facilities to ensure acknowledgement of the requirement to cease MTSA

related operations after June 30, 2004. As soon as practicable, COTPs will issue letters notifying the owners or operators of these facilities that they will be prohibited from performing MTSA related operations after June 30, 2004, unless the facilities achieve compliance. On July 1, 2004, COTPs will issue COTP orders to facility owners or operators prohibiting MTSA related operations at facilities that do not possess one of the four documents listed in paragraph 11.4.1.

11.11 Enforcement Philosophy

11.11.1. The Coast Guard will work cooperatively with facilities while verifying compliance with their FSP. COTPs are strongly encouraged to enhance compliance through proactive engagement with industry. It is very important that the COTP and facility inspection teams work together with industry personnel so that meaningful security improvements are made permanent. For facilities that are making a good faith effort to implement their FSPs and are in substantial compliance, on-the-spot corrections of minor deficiencies may be appropriate. For those facilities that are not in substantial compliance, progressive enforcement tools may be used such as NOVs and civil penalties.

11.11.2. The four key steps of FSP verification are to (1) ensure facilities comply with their FSP; (2) ensure the approved FSP/ASP adequately addresses the performance-based criteria as outlined in 33 CFR Part 105; (3) ensure the accuracy of the Facility Security Assessment (FSA); and (4) ensure that measures are in place to adequately address the vulnerabilities.

11.11.3. The COTP should consider the entire scale of enforcement tools available when determining enforcement actions, such as documenting an initial, minor violation in a Letter of Warning (LOW), with subsequent violations documented in NOVs, civil penalties, or criminal penalties. Enforcement actions are not appropriate in cases where the facility is operating in accordance with their FSP/ASP, but when the FSP / ASP is determined to inadequately address the performance standards in the regulations. In these cases, the COTP should follow the amendment guidance found in 33 CFR 105.415. The COTP must consult the cognizant District Legal Officer prior to initiating criminal penalty action.

11.12. Enforcement Cycle and Control Actions

11.12.1. From July 1, 2004, until December 31, 2004, the Coast Guard will verify that approved security programs have been implemented by MTSA regulated facilities. Thereafter, security program enforcement will be scheduled to coincide with annual inspections. Any deficiencies noted during an intervening inspection must be addressed immediately.

11.12.2. If the facility cannot implement its FSP because of unavoidable delays involved with physical improvements, it must identify and implement equivalent measures pending the installation of the permanent equipment as outlined in paragraph 11.6. If the facility has not implemented adequate equivalent measures to the satisfaction of the COTP, the COTP should take appropriate control actions.

11.12.3. COTPs may verify facility implementation on any facility at any time and should prioritize verification efforts based on risk (e.g., high risk cargo stored in a high consequence location). See enclosure (2) for specific guidance. However, by law, facilities are not required to implement their security plans until July 1, 2004. This includes those facilities that are operating under an approved ASP, an approved FSP, an interim approved FSP, or by LOA.

11.12.4. The COTP will document the initial and subsequent compliance visits using the MTSA Facility Compliance Guide located in enclosure (10) and document appropriately in MISLE using the procedures outlined in the document titled *Documentation of Maritime Security Activities for Domestic Facilities (MTSA) User Guide*, located at http://mislenet.osc.uscg.mil/user_guides.aspx.

11.12.5. A MTSA compliance matrix, Addendum (3) to this enclosure, has been developed to provide guidance for initiating control, compliance, and penalty actions. This matrix is intended as a tool to be used by the COTP/OCMI to evaluate a facility's compliance with the requirements of MTSA. This tool is recommendatory in nature and is designed to provide consistency in evaluating a facility's level of compliance and determining appropriate control measures. The categories follow the items identified in the MTSA Facility Compliance Guide for facility compliance examinations. The guide should be used to capture the summary results from the specific items verified and documented in the checklist. Available enforcement options are readily assessable for each category. While these individual controls for each category can be applied as a means of addressing the risk represented by non-compliance, the cumulative severity of the non-compliant items should also be weighed when identifying the appropriate level of control. For facilities in significant non-compliance, a suspension or revocation of the FSP should be strongly considered in addition to restriction of any vessel operations. While the FSP may describe measures needed to be in compliance with the applicable standard, it could be concluded that the facility owner/operator is unable to effectively implement that plan and a significant review may be needed.

11.12.6. Because a facility operating under an ILA or LOA must implement its submitted FSP in its entirety, its compliance should be verified in the same fashion as a facility with an approved FSP.

11.12.7. When a facility is in compliance with its FSP but the measures in the FSP (whether approved or awaiting approval) are not sufficient to reduce identified vulnerabilities, the COTP should require the owner or operator to amend the FSP. The COTP must do this in writing and allow the owner or operator at least 60 days to propose amendments. Until amendments are approved, the owner or operator shall ensure appropriate temporary security measures are implemented to the satisfaction of the COTP. Amendments must be submitted to the COTP for approval in accordance with 33 CFR 105.415. In those cases where the FSP has been implemented but must be amended, no penalty action should be taken.

11.13 Additional Compliance Checks for Facilities Receiving Vessels Subject to SOLAS Chapter XI-2 and ISPS

11.13.1. Port State Control (PSC) Boarding Officers conducting dockside PSC examinations should observe and document important security measures while entering and departing facilities used by vessels subject to SOLAS. The PSC Boarding Officers are not expected to perform a complete exam, but should take note of the specific security measures as listed below. If the PSC Boarding Officers observe a lack of security or there is a perceived lack of security at a facility, the PSC Boarding Officers should alert the unit's Facility Security personnel for follow on examinations or spot checks. At a minimum, PSC Boarding Officers should note that:

- Access control measures are in place at facility entrances
- The facility is checking the identity of people entering the facility
- Signs are conspicuously posted describing security measures
- Security personnel are vigilant and alert
- Security personnel are equipped with adequate communications

- The facility, in liaison with the vessel, is escorting visitors and delivery vehicles on the facility, as appropriate
- The facility, in liaison with the vessel, is checking cargo and/or vessel stores, as appropriate
- Restricted areas are marked and additional security measures are in place, as appropriate
- Declarations of Security are being completed, as appropriate
- Security measures for monitoring security, such as lighting, security patrols, etc., are in use, as appropriate

11.14 Suspending Operations

11.14.1. If the COTP determines that a facility must suspend operations, the COTP should issue a written COTP order directing the facility to suspend 33 CFR 105 regulated operations. If the violations are so egregious that the entire port is at risk, the facility may be shut down in its entirety.

11.14.2. Controls may also span the spectrum available to the COTP, from restricting specific facility operations to suspending operations outright with a COTP order. The Vessel/Facility Compliance Matrix is a tool for COTP/OCMI's in determining appropriate control and enforcement options. The COTP may also suspend and revoke the FSP, thereby making the facility ineligible to perform MTSA related operations.

11.15 Intermittent Operations

11.15.1. Many facilities perform MTSA regulated functions intermittently and may implement variable security measures based on the risk it presents while not actively receiving MTSA regulated vessels or storing cargo intended for MTSA regulated vessels. The FSA and FSP must address the variable security measures the facility will use as well as those measures that it will use prior to resuming full MTSA regulated operations, such as sweeping the facility after reestablishing perimeter control. An example of intermittent operations would be a facility regulated by 33 CFR Part 105 because it receives vessels subject to SOLAS. However, when the facility is receiving non-SOLAS vessels or vessels not regulated by 33 CFR Part 104, it may significantly reduce its security measures provided the threat of a Transportation Security Incident (TSI) is low.

11.16 Lower Consequence Plan Review Methodology

11.16.1. The Coast Guard recognizes that facilities regulated by 33 CFR 105 pose varying levels of risk. Therefore the Coast Guard developed a "lower consequence" methodology to review and approve security plans for facilities that handle only dry bulk commodities, or other wise pose lower levels of risk due to their operations or their geographic locations. These facilities are required to complete an assessment of their operation, develop mitigating strategies, and write a plan but to a lesser extent of detail and process. The low consequence methodology was developed in recognition of the lower risk associated with such facilities and allows greater flexibility in the types of security measures that may be employed. Security plans that were reviewed using the lower consequence methodology comply with each section of the regulations and include all 18 general elements of a facility security plan, but may contain less detail. Reviewers at the NFSPRC are utilizing this methodology during Stage II reviews. There are two ways to determine if the low consequence methodology was used. When the NFSPRC began using the low consequence methodology, the internal comment sheet stated the facility was considered a lower

consequence facility. Subsequently the Stage 2 check sheet was annotated to show the facility security plan was reviewed using the low consequence methodology.

11.17 Declaration of Security (DoS) Applicability

11.17.1. The following guidance is provided to ensure consistency in the proper utilization of the DoS.

11.17.2. At MARSEC LEVEL 1: Only cruise ships (as defined by 33 CFR 101.105) and manned vessels carrying CDCs (as defined by 33 CFR 101.105) are required to complete a DoS *if* there is a "vessel-to-vessel activity" or a "vessel-to-facility interface" (as defined by 33 CFR 101.105). However, if there are no actions that meet the definitions of "vessel-to-vessel activity" or a "vessel-to-facility interface", then no DoS is required.

11.17.3. At MARSEC LEVELS 2 and 3: All manned vessels to which 33 CFR Part 104 applies are required to complete a DoS *if* there is a "vessel-to-vessel activity" or a "vessel-to-facility interface" (as defined by 33 CFR 101.105). This would include passenger barges, permissively manned barges and uninspected towing vessels regardless of whether they are towing. However, if there are no actions that meet the definitions of "vessel-to-vessel activity" or a "vessel-to-facility interface", then a DoS is not required, i.e., if the vessel simply moors at the facility, but there is no movement of persons, cargo, vessel stores, or there are no port services to or from the vessel being provided, a DoS is not required. Dropping off or picking up a barge at a facility does not constitute a "vessel-to-facility interface".

11.17.4. At all MARSEC LEVELS: All unmanned vessels to which 33 CFR Part 104 applies are *not* required to complete a DoS. Other provisions of the regulations require owner and operators of unmanned barges to take into account the secure transfer of unmanned vessels from towing vessel to facilities. An unmanned barge remains unmanned regardless of tankermen or towing vessel crew working aboard the vessel.

11.17.5. A "Declaration of Security (DoS) Applicability Decision Tool" is located in addendum (2) of this enclosure. It provides a graphic representation further delineating DoS applicability.

11.18 Facilities with Megayachts

11.18.1. There are marinas, restaurants, and fueling docks that receive small vessels that travel on international routes. The amount of time these vessels remain at these facilities varies between a few hours to a few weeks. Based upon the above, the following policy guidance is in effect:

11.18.2. Each marina or facility that receives foreign flagged SOLAS passenger vessels and yachts that are equal to or greater than 500 gross tonnage, carrying at least one passenger for hire on international voyage(s), are required to comply with 33 CFR Part 105.

11.18.3. Each marina or facility that receives foreign flagged SOLAS passenger vessels and yachts that are less than 500 gross tonnage, carrying more than twelve (12) but less than 151 passengers, with at least one passenger for hire (including voyages without a specified destination), are required to have an approved security plan if the vessel described above embarks, disembarks, or has passengers on board

while at the facility. (See 33 CFR 105.310, 33 CFR 105.410, 33 CFR 101.145 and NVIC 04-03 enclosure (3))

11.18.4. Each marina or facility that receives foreign flagged passenger vessels and yachts that are less than 500 gross tonnage, carrying twelve (12) or less passengers for hire on domestic or international voyage(s), are not required to have a facility security plan.

11.19 Remote Facilities

11.19.1. The regulations in 33 CFR 105.105 provide an exemption provision for an isolated facility that receives material(s) regulated by 33 CFR Parts 126 or 154 by vessel if there is no road access to the facility. By applying the "isolated facility" exemption provision in 33 CFR 101.105 (c) (5) to isolated oil/cargo/container facilities regulated by 33 CFR Parts 126 and 154, the cognizant COTP can make a recommendation for exemption to the District Commander based on all of the following criteria:

- The risk of a Transportation Security Incident (TSI) is low
- The consequences of a TSI (loss of life, economic impact, or environmental harm) are low
- The community where the facility is located is not visited by passenger vessels with more than 150 passengers
- The facility is inaccessible by road from other communities, domestic or foreign
- The facility does not conduct secondary transfers in bulk of the commodities it receives, i.e., it does not serve as a staging area for the consolidation and transshipment of dangerous cargo or oil (250 barrels) to other ports via commercial vessels
- The facility receives cargoes by vessel(s) only

11.19.2. Facilities that meet some, but not all, of the criteria may forward a request for a waiver under 33 CFR 105.130 to Commandant (G-MP) asking for permission to waive the requirements of 33 CFR Part 105.

11.20 Facilities Handling Cargoes Regulated by 46 CFR Part 148

11.20.1. The Coast Guard has conducted a careful review of the cargoes listed in 46 CFR Part 148 and the IMO Code of Safe Practice for Solid Bulk Cargoes (BC Code) and has determined that certain cargoes pose a lower risk of causing a transportation security incident. A vessel that handles such cargoes is not subject to 33 CFR Subchapter H unless there is another applicability factor. As such, the Coast Guard is exempting a facility (exemption is not applicable to vessels) that only receives the following cargoes, listed in either 46 CFR Part 148 or the BC Code, from a vessel not otherwise subject to 33 CFR Part 104.

11.20.2. The following cargoes as they appear in the Bulk Cargo Code:

- Brown Coal Briquettes (Lignite)
- Calcined Pyrites (Pyritic ash, Fly ash)
- Charcoal
- Coal
- Direct Reduced Iron (Hot & Cold molded)
- Ferrosilicon, containing 25% to 30% silicon or 90% or more silicon (including briquettes)*****
- Fluorspar (Calcium Fluoride)

- Magnesia (unslaked)
- Metal Sulphide Concentrates
- Peat Moss
- Pitch Prill (Prilled Coal Tar, Pencil Pitch)
- Silicomanganese (with a silicon content of 25% or more)*****
- Vanadium Ore
- Woodchips
- Wood Pulp Pellets

11.20.3. The following cargoes as they appear in 46 CFR Part 148:

- Ferrophosphorus
- Lime (unslaked)
- Petroleum coke (calcined)
- Petroleum coke (uncalcined)
- Sawdust

11.21 Facilities that receive drilling mud

11.21.1. After careful review by the U.S. Coast Guard, it has been determined that drilling mud poses a low risk of causing a transportation security incident. Therefore, the Coast Guard is exempting vessels that handle drilling mud from the requirements of 33 CFR Part 104 unless another applicability factor is involved. The Coast Guard is also exempting facilities that receive drilling mud from a vessel not subject to 33 CFR Part 104 unless another applicability factor is involved. However, these exempted vessels and facilities remain subject to 33 CFR Parts 101 and 103.

11.22 Checking Identification and Performing Passenger, Baggage, Vehicle Screening

11.22.1. When used in concert, 33 CFR 105.106, 33 CFR 105.110, 33 CFR 105.285 (a)(5), (b) and (c) provide an alternative to the identification check and passenger screening requirements for facilities that serve passenger vessels and ferries. Facilities that have implemented these sections of the regulations in their facility security plan are not required to check the identification of passengers or screen passengers, baggage, or personal effects at the rate specified in the applicable MARSEC Directive.

11.22.2. Alternative Security Programs, such as those under the American Gaming Association and the Passenger Vessel Association, have also implemented 33 CFR 105.106, 33 CFR 105.110, 33 CFR 105.285 (a)(5), (b) and (c). Facilities implementing these ASPs are not required to check the identification of passengers or screen passengers, baggage, or personal effects at the rate specified in the applicable MARSEC Directive.

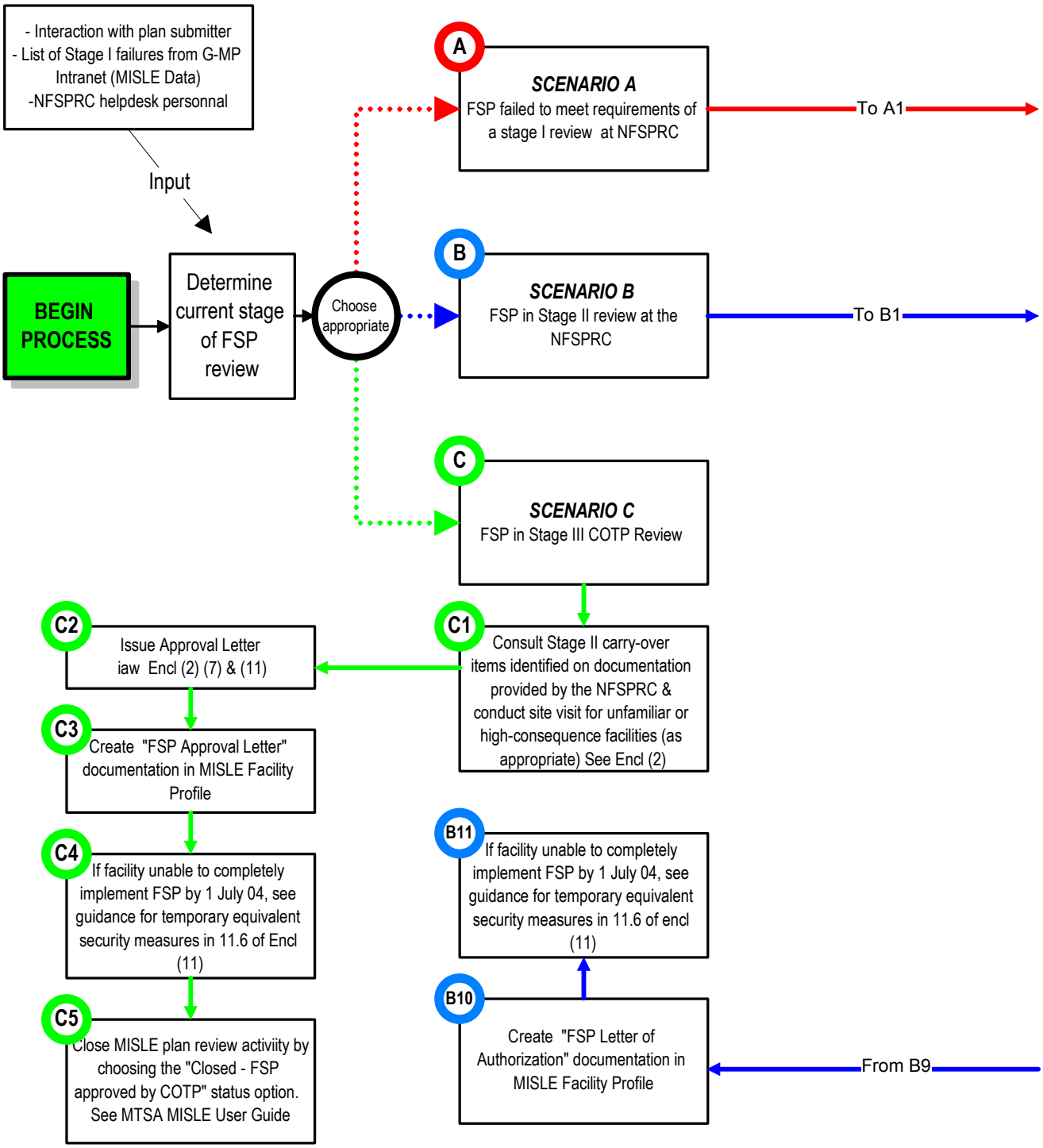
11.22.3. At this time there is no alternative for vehicle screening. All facilities must screen vehicles at the rate specified in the applicable MARSEC Directive.

ADDENDUM (1) to ENCLOSURE (11)

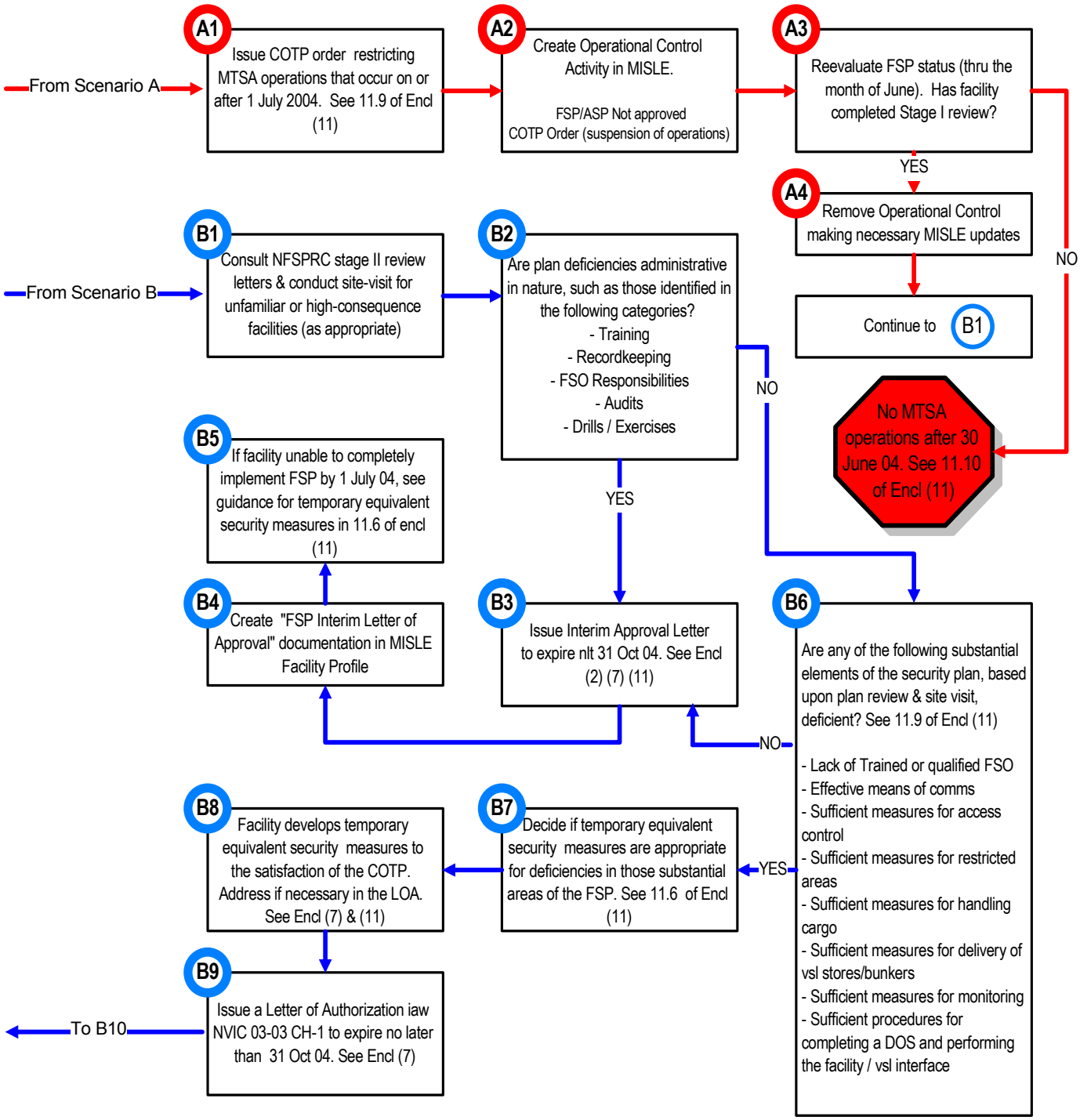
Decision Tool for issuing Letters of Approval, Interim Letters of Approval, and Letters of Authorization

This Addendum contains a single flow-chart covering two pages (14 & 15)

Decision Tool for issuing Letters of Approval, Interim Letters of Approval, and Letters of Authorization
Page (1)



Decision Tool for issuing Letters of Approval, Interim Letters of Approval, and Letters of Authorization
Page (2)



ADDENDUM (2) to ENCLOSURE (11)

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

DECLARATION OF SECURITY (DoS) APPLICABILITY DECISION TOOL

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

Step 1 – Utilizing Table 1, assign a category (**CAT**) for each vessel or facility involved in the interface[1].

TABLE 1 - VESSEL / FACILITY CATEGORY DECISION MATRIX

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

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

TABLE 2 – DOS INTERFACE DECISION MATRIX

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

Table Legend

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

[1] Interface means to engage in the transfer or movement of persons, cargo, stores, or provisions between a vessel and facility or a vessel and another vessel. See 33 CFR 101.105.
[2] Vessels are considered to be "CDC" if they are carrying cargoes listed in 33 CFR 160.204.
[3] Vessels are considered "Manned" if a crew is required as per their Certificate of Inspection (COI). An unmanned barge remains "unmanned" regardless of Tankermen or towing vessel crew working aboard the vessel.

ADDENDUM (3) to ENCLOSURE (11)

MTSA Compliance Matrix

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

CODES FOR CONTROL & COMPLIANCE MEASURES

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

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

CODES FOR PENALTY MEASURES

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