Subject: CH-1 to NVIC 11-02, IMPLEMENTATION GUIDANCE FOR THE MARITIME TRANSPORTATION SECURITY ACT (MTSA) REGULATIONS FOR FACILITIES

Ref: (a) 33 CFR Part 101
(b) 33 CFR Part 103
(c) 33 CFR Part 105

1. PURPOSE. This Navigation and Vessel Inspection Circular (NVIC) significantly revises NVIC 11-02. Significant changes include concepts of operations and guidelines for the implementation of the Maritime Transportation Security Act (MTSA) regulations applicable to facilities. This NVIC details the Facility Security Plan (FSP) and Alternative Security Program (ASP) review processes, FSP/ASP verification inspections, and general enforcement guidance for non-compliance. It is intended for use by Captain of the Port (COTP) personnel as well as owners/operators of affected facilities as an aid in complying with MTSA. Enclosure (5) "Guidance on Assessing Facility Security Measures" of NVIC 11-02 has been retained unchanged and is included as Enclosure (9) in this CH-1.

2. ACTION.

a. Captains of the Port (COTP) shall bring this circular to the attention of marine interests within their areas of responsibility. This circular will be distributed by electronic means only and is available on the World Wide Web at: http://www.uscg.mil/hq/g-m/index.htm.

b. The Coast Guard intends to use this guidance during the review and verification of FSP/ASPs. Facility owners and operators may use this circular as guidance to develop their FSP/ASP and to prepare for verification visits and compliance inspections.

3. BACKGROUND.

a. The purpose of the MTSA regulations found in 33 CFR 105 is to require security measures for facilities in order to reduce risk and to mitigate the results of an act that threatens the security of personnel, the facility, and the public. The Coast Guard is responsible for verifying that each affected facility complies with the MTSA regulations. Facilities that are not specifically regulated under part 105 may be subject to the requirements of 33 CFR 103.

b. The Coast Guard has traditionally focused inspections on waterfront portions of those facilities transferring oil or hazardous materials (33 CFR 126, 127, and 154). These inspections tended to include a cursory security inspection as previous regulations focused on hazardous material transfer safety only. The MTSA regulations found in 33 CFR 105 greatly expands Coast Guard inspection/oversight responsibilities in two significant areas. First, the definition

of applicable facilities is more encompassing and adds approximately 1,000 additional facilities not traditionally regulated by the Coast Guard including barge fleeting facilities and terminals that receive certain vessels over 100 GT on international voyages. Secondly, MTSA greatly expands Coast Guard jurisdictional boundaries to well beyond the traditional "first valve within containment" and may encompass the entire facility complex.

4. DISCUSSION.

   a. Enclosures (1) through (9) provide guidance to ensure consistency in the FSP/ASP review and verification process and enforcement actions to ensure compliance with FSP submission and implementation. The purpose of the FSP/ASP review and verification process is to ensure nationwide consistency in the application of the MTSA regulations. The review and verification process consists of three stages. Stages I and II determine that a FSP/ASP meets the elements of the regulations. Stage III verifies the submitted FSP/ASP plans are adequate for approval.

   b. Inspection checklists will be released at a later date and will be intended for both COTPs and facility owners/operators to ensure consistency during post 1 July 2004 facility compliance examinations. Facilities must comply with their FSP/ASP by July 1, 2004.

   c. Information regarding the intent of the regulations will be available on the G-MP MTSA website at http://www.uscg.mil/hq/g-m/mp/mtsa.shtml. This information was taken from the preamble discussion in the Final Rule and provides insight that led to the development of the regulations. It is also included to further assist inspectors and industry personnel during security examinations. It is highly recommended that both COTPs and facility owners/operators become familiar with the information contained herein.

5. IMPLEMENTATION.

   a. The implementation of MTSA requirements found in 33 CFR 105 will be executed in three distinct phases. These phases include:

      - FSP Development & Submission Phase (thru December 31, 2003)
      - FSP Review & Approval Phase (January 1, 2004, thru June 30, 2004)
      - Enforcement Phase (July 1, 2004 and beyond)

      This "phased-in" methodology allows for rapid deployment of critical regulatory provisions.

   b. Enclosure (1) is a flow chart of the MTSA plan review process methodology for facilities from the initial FSP/ASP submission to the implementation stages.

c. Enclosure (2) provides a detailed overview of the plan review process, implementation philosophy, and enforcement guidance. There are two critical dates associated with the FSP review and implementation process. A facility submitting a FSP after the December 31, 2003 deadline is subject to civil penalty action. A facility that is not operating under an approved FSP or ASP or pursuant to a Letter of Authorization after June 30, 2004 may be subject to additional control and compliance measures including suspension of facility operations.

d. Enclosure (3) is the Stage I review form utilized by plan review personnel.

e. Enclosure (4) is the Stage II review form utilized by plan review personnel.

f. Enclosure (5) is the ASP review form utilized by plan review personnel.

g. Enclosure (6) is the Stage III review form for COTPs.

h. Enclosure (7) contains sample plan review-related letters for use by COTPs and the FSP Central Review Office.

i. Enclosure (8) contains amplified information concerning MTSA applicability to facilities.

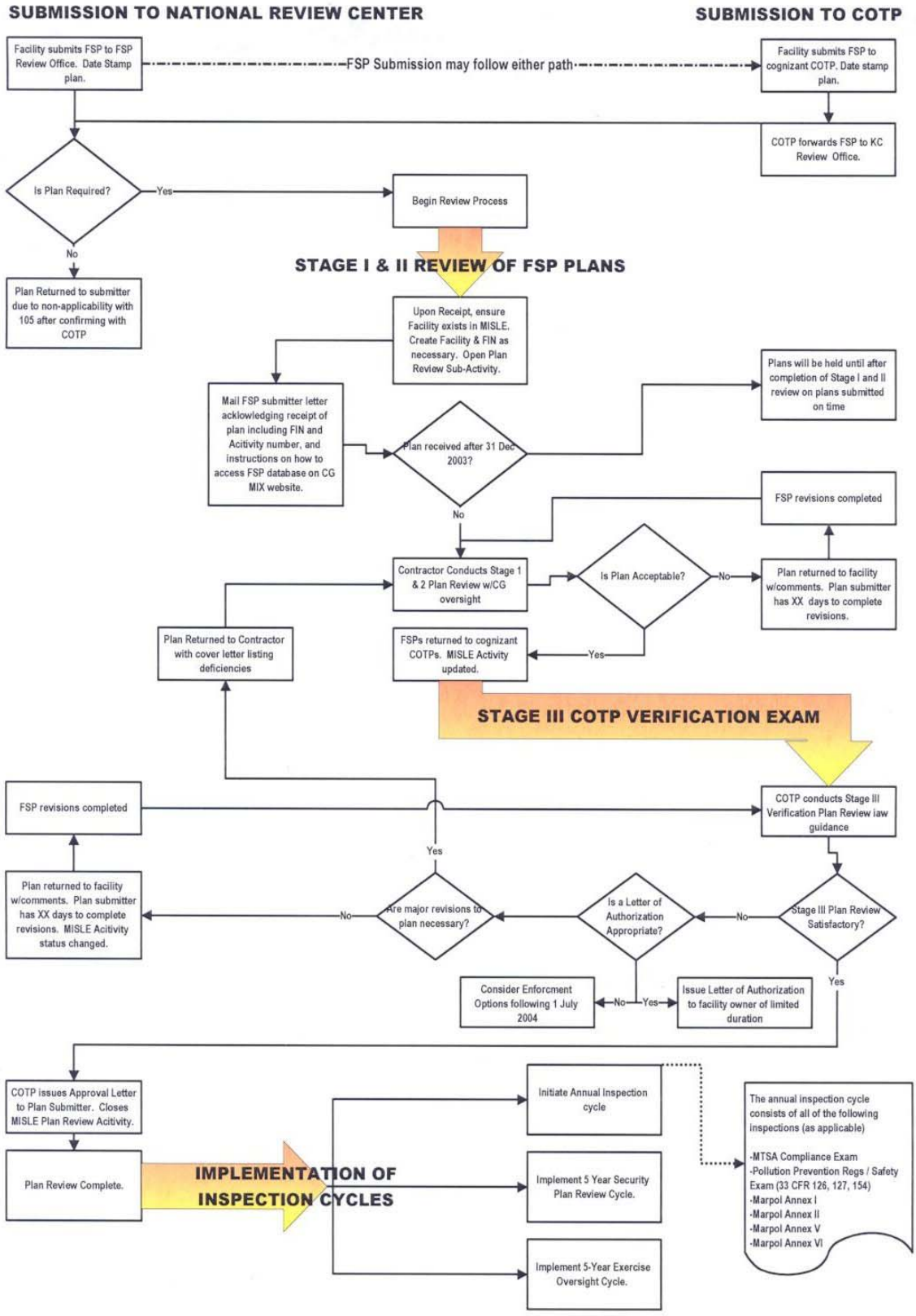
j. Enclosure (9) is "Guidance on Assessing Facility Security Measures"

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

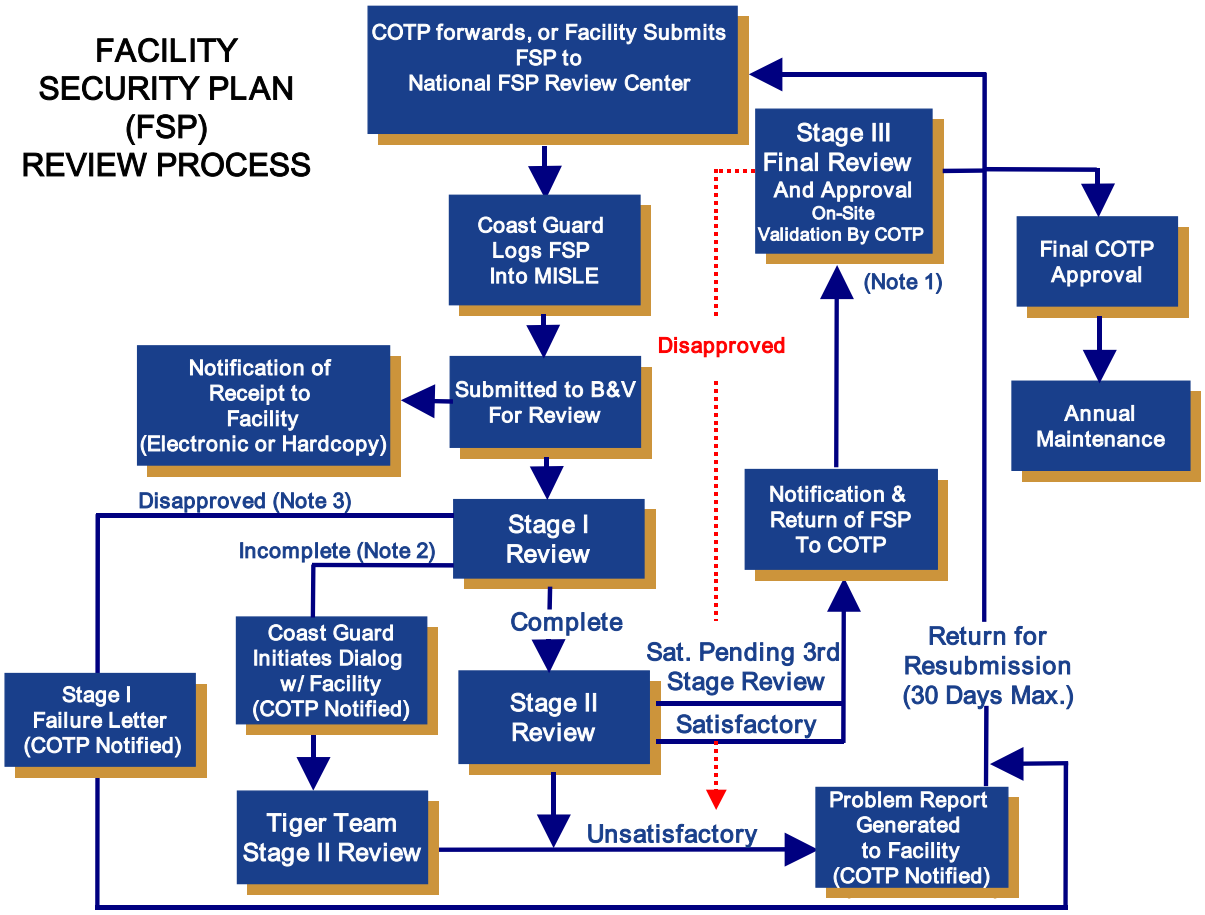
//ss//

Encl: (1) Plan Review Process Methodology Flowchart
(2) MTSA FSP/ASP Implementation Process Methodology
(3) Stage I Checklist
(4) Stage II Checklist
(5) ASP Checklist
(6) Stage III Checklist
(7) Sample Plan Review-Related Letters
(8) Applicability Guidance
(9) Guidance on Assessing Facility Security Measures

Facility Security Plan Methodology



ASP Submission Flow Chart [Under Development]



NOTES

1) Stage III includes; review of the assessment report, and any carry over items forwarded by the National FSP Review Center
2) One regulation review topic other than failure to submit FSA or 6025 is incomplete and proceeds to Tiger Team Stage II Review
3) No FSA report or 6025 submitted with plan or two or more of the other regulation review topic are incomplete, then the plan will be returned disapproved

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 July 1, 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, plans that have not completed Stage III review by July 1, 2004, with the following conditions:
    - Plan was submitted by December 31, 2003, and
    - the facility owner has met all plan correction deadlines
- For facilities not in service by December 31, 2003, and 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.

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 July 1, 2004.

2.3 Implementation Methodology

2.3.1. The implementation of MTSA[1] requirements found in 33 CFR 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** (thru December 31, 2003) - Key components of this period include:

- Facilities to which 33 CFR 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].
- COTPs shall compile a list of those facilities to which 33 CFR 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 with contractor support at offices located in Kansas City. FSPs will be reviewed in the order in which they are received.

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

- 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 FSP owner for revision.
- 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.
- In the event a FSP is not approved by July 1, 2004, the COTP may issue a Letter of Authorization to operate until the FSP is approved.
- The COTP will communicate with facilities identified as not having submitted an FSP in accordance with the regulations. Civil penalty action may be warranted for those facilities not complying with plan submission requirements.

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

- All facilities must be in full compliance with 33 CFR 105.

[1] Unless otherwise noted, references to the Marine Transportation Safety Act of 2002 (MTSA) regulations include all requirements of 33 CFR 101-106 (as applicable).
[2]The "National FSP Review Center" will be referred to as the "Center" throughout this enclosure.
[3] MISLE is the central computer based database in which most CG activities are captured.

- Facilities operating with a FSP must have either an Approval Letter or a Letter of Authorization issued by the COTP.
- Facilities operating under an approved 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 all stages 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.
- Civil penalty action and/or suspension of operations may be warranted for those facilities not complying with plan submission and compliance requirements.

2.4 Facility Security Plan (FSP) Review

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. Stage I and II consists of an in-depth review of the submitted plan by Center personnel, ensuring the plan meets all regulatory requirements. Stage III review is designed to ensure overall *adequacy* of the plan by the COTP, 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. COTP's will make every effort to complete all stages of the plan review process by 1 July 2004. This date is critical, as facilities must comply with their security plan by this date 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 Captain of the Port (COTP) by December 31, 2003. As the preferred method, facilities may submit their plans directly to:

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

2.5.2. COTPs shall forward all received plans to the Center utilizing an express courier (e.g. FEDEX or UPS) immediately upon receipt, logging the 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. COTPs 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
- FIN
- OPFAC

2.5.3. Center personnel will screen all plans upon receipt to determine *applicability* to 33 CFR 105 and will review only those as required by that part. Center personnel will liaison with the cognizant COTP's prior to final determinations. Plans will be returned to the submitter following a "non-applicability" determination made by Center personnel. Enclosure (8) provides additional policies to define an individual facility's regulated areas.

2.6 Stage I & 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 rare case that a facility 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 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 December 31, 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. Plans will be reviewed in the order received.

2.6.4. Following a successful 2.5.3. screening, a plan will undergo a Stage I review to ensure the required sections are properly included/addressed. Center personnel will utilize the review form incorporated as enclosure (3). Major deficiencies noted during Stage I review will require the plan to be resubmitted with corrections prior to Stage II review. Major deficiencies include:

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

- Two or more "incomplete" FSP content requirements (for 1-16 enclosure (3)),
- 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 2.6.6. of this chapter 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 every regulatory requirement. 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. A sample letter is contained as a part of enclosure (7). COTP's will receive courtesy copies of all Stage I failure letters.

2.7 Stage III COTP Review and Approval

2.7.1. Following a successful Stage II review, all FSPs will be mailed to the cognizant COTPs for further 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 should deficiencies be noted during the Stage III review process:

- Inform the plan owner via letter of the noted deficiencies and the timeframe for submitting revisions, or;
- return plan to the Center for another Stage II review with a letter detailing deficiencies found.

This 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.

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

2.7.5. An FSP in Stage III review not meeting all requirements will be returned to the FSP owner for corrective action. The COTP may issue the facility a Letter of Authorization, allowing the facility to continue to operate pending approval. A sample letter is contained as part of enclosure (7).

2.8 Alternative Security Program

2.8.1. An Alternative Security Program (ASP) is 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. Members in good standing in these organizations may implement the approved 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:

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

2.8.3. Facilities are *encouraged* 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.

2.8.4. Once the Center receives the information listed above, a 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 CG-6025 is reviewed and the required MISLE entries completed, a copy of the letter and the CG-6025 will be sent to the COTP. This review is conducted in accordance with the ASP Review Form, enclosure (5).

2.8.6. The COTP reviews the specific facility security plan for appropriate application of the approved ASP. This review is conducted in accordance with the FSP Stage III review form, enclosure (6) of this NVIC. If the CG-6025 has not identified and addressed all vulnerabilities, it will be corrected and resubmitted to the Center.

2.9 Waivers and Equivalencies

2.9.1. Waiver requests 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 equivalence requests along with recommendations to HQ 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 NFSPRC and the COTP receiving a copy.

2.9.5. Approved waivers and equivalencies should be kept on file with the FSP. These will also be available 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 the implementation of MTSA imposes numerous additional security regulations 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. MTSA requirements will be verified by Coast Guard personnel on an annual basis in conjunction with other required examinations. There are three pieces to MTSA verification following the implementation of MTSA beginning on 1 July 2004. These include MTSA Compliance examinations, exercise oversights and plan reviews.

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

- MTSA (33 CFR 101, 103, 105)
- Pollution Prevention / Safety (33 CFR 126, 127, 154)
- MARPOL Annex I, II, V, VI[6] (33 CFR 158)

2.10.3. Annual MTSA examinations will measure compliance with requirements in 33 CFR 101, 103 and 105. This examination specifically audits a facility's compliance with their approved FSP. G-MOC is developing a compliance inspection form (Enclosure (10)) that will serve as further guidance. This form will be provided to all Coast Guard facility inspectors to ensure consistency during these examinations. COTP's will utilize a

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

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 COTP's will conduct compliance inspections 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 MTSA compliance exam later in the period to coincide with other required facility inspections (e.g. MARPOL, 33 CFR 126, 127, 154).

2.10.4. FSP approval letters are only valid for a 5-year period; requiring security plans to complete a new review and approval process. This process is currently under development and it is anticipated that all 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 on or before December 31, 2003, facility owners or operators must submit their required documents to the cognizant COTP or National FSP Review 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 105.

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

2.13 MISLE Methodologies

2.13.1. Enhancements have been made to the MISLE database to assist in tracking the progress of 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 thru use of the MARS program. Guidance on MARS use will be made available to COTPs through separate correspondence.

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

(18) Facility Vulnerability and Security Measures Summary (Form CG-6025). *A completed form CG-6025 has been submitted.*	☐	☐

Item:	***Incomplete Reason:***

Note: *If two or more of content requirements 1-16 are incomplete, then the FSP is to be returned to the originator for correction before going to stage 2 review. If one content requirement for 17 or 18 is incomplete, then the FSP is to be returned to the originator for correction before going to stage 2 review.*

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
(19) 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 a 3rd Stage 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.	☐	☐	☐	☐
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				

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
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**.				
(20) 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,				

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
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.				
(21) 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 response? 3.3 Does the FSP identify exercises that test the entire security program and include substantial and active participation of FSOs?	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐	☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐ ☐

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
(22) 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 Facility Security Plan (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.	☐	☐	☐	☐
(23) 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 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	☐	☐	☐	☐

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
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.	☐	☐	☐	☐
(24) 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**?	☐	☐	☐	☐
(25) 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; 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 DOSs as required in	☐	☐	☐	☐

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
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 DOSs be kept with the Facility Security Plan?	☐	☐	☐	☐
8. Does the FSP contain procedures to be used when the COTP requires additional DOS implementation?				
(26) 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?	☐	☐	☐	☐
(27) 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.	☐	☐	☐	☐
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?	☐	☐	☐	☐
(28) Security measures for access control;				

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

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

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
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.				
(29) 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 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;	☐	☐	☐	☐

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

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
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.				
(30) 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 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,	☐	☐	☐	☐

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
of all dangerous goods or hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods or hazardous substances;				
1.10 Be able to check cargo entering the facility for dangerous substances and devices at the rate specified in the approved Facility Security Plan (FSP). Means to check cargo include:				
1.10.1 Visual examination;	☐	☐	☐	☐
1.10.2 Physical examination;	☐	☐	☐	☐
1.10.3 Detection devices, such as scanners;	☐	☐	☐	☐
1.10.4 Canines.	☐	☐	☐	☐
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 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.				

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
(31) 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?	☐	☐	☐	☐
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?				
(32) Security measures for monitoring;				

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

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
(33) 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?				
(34) 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?	☐	☐	☐	☐
(35) 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:				
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?	☐	☐	☐	☐

FSP Content Requirements:	*Satisfactory*	*Not Satisfactory*	*Pending 3rd Stage*	*Not Applicable*
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?				
(36) Facility Vulnerability and Security Measures Summary (Form CG-6025).				
Appendix A to Part 105--Facility Vulnerability and Security Measures 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?	☐	☐	☐	☐

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

Item:	***Incomplete Reason:***

ASP Content Requirements:	*Complete*	*Incomplete*
(37) Implementation Letter; *Does the plan have an implementation letter for an approved Alternate Security Program (ASP)?*	☐	☐
(38) Non-Government Organizations; *Does the plan indicate they are a member of any Non-Government Organizations (NGO)?*	☐	☐
(39) Facility Vulnerability and Security Measures Summary (Form CG-6025). **Appendix A to Part 105--Facility Vulnerability and Security Measures Summary (Form CG-6025)** *(1) Has Form CG-6025 been completed?* *(2) Are the mitigation strategies appropriate and adequate for the identified vulnerabilities?*	☐ ☐	☐ ☐

Item:	***Incomplete Reason:***

FSP Content Requirements:	*Complete*	*Incomplete*
(40) (FSP/ASP) Review and evaluate Stage 2 Review form and address pending items. *This may range from phone call to facility to on-site facility visit*	☐	☐
(41) (FSP Only) 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.*	☐	☐
(42) (FSP Only) 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.*	☐	☐
(43) (ASP Only) Obtain list of FSO and 24 hour contact information. *This information is typically not available through the ASP, COTP's should obtain this information and update MISLE.*	☐	☐
(44) (FSP Only) Approval letter signed and delivered. *For plans satisfactorily completing items 1-4 above (as appropriate)*	☐	☐
(45) (FSP Only) 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:*

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

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

SSIC
Date
MISLE Activity #

XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE PLAN RECEIPT LETTER

Dear Mr./Ms. XXXX:

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

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

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

Sincerely,

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

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

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

SSIC
Date
MISLE Activity #

XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE STAGE I FAILURE LETTER

Dear Mr./Ms. XXXX:

We have completed a Stage I review of your submitted facility security plan dated *[date]* for *[Company Name]*. Regrettably, your plan does not meet the requirements as outlined in 33 CFR 105 and is being returned for correction. Below is a summary of 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, we will forward your plan for further review.

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

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

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

Sincerely,

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

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

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

SSIC
Date
MISLE Activity #

XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE STAGE II PROBLEM LETTER

Dear Mr./Ms. XXXX:

We have completed a Stage II review of your submitted facility security plan dated *[date]* for *[Company Name]*. Unfortunately, your plan does not meet the requirements as outlined in 33 CFR 105. Below 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 for further review.

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

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

Sincerely,

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

U.S. Department of Homeland Security

United States Coast Guard
Commandant
United States Coast Guard

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

SSIC
Date
MISLE Activity #

XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE LETTER OF AUTHORIZATION TO OPERATE LETTER

Dear Mr./Ms. XXXX:

The facility security plan (FSP) for [*Facility Name]*, submitted to meet the requirements of Title 33 Code of Federal Regulations (CFR) Part 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 *[date / up to one year]*, at which time the Coast Guard will reevaluate the status and progress of your plan submission.

Commencing July 1, 2004, [*Facility Name]* must operate in full compliance with their submitted FSP and any additional requirements contained in 33 CFR 105. You are reminded that any deviation from this submitted plan requires immediate notification to this office. Your facility security plan is sensitive security information and 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
Commandant
United States Coast Guard

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

SSIC
Date
MISLE Activity #

XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE PLAN APPROVAL LETTER

Dear Mr./Ms. XXXX:

The facility security plan for [*Facility Name]*, submitted to meet the requirements of Title 33 Code of Federal Regulations (CFR) Part 105, is approved.

Commencing July 1, 2004, [*Company/Facility Name]* must operate in compliance with this approved security plan and any additional requirements contained in 33 CFR 105. You are reminded that any deviation from this approved plan is required to be immediately reported 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.

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 Part 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

8.1 Applicability Job Aid

8.1.1. On August 27th and 28th, 2003, a working group met to discuss develop regulatory models for the application of the MTSA security regulations. This has proven to be a difficult issue 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 EPA, trade associations, and industry representatives.

8.1.2. 33 CFR 105.105 states the applicability for facilities. The enclosed satellite photographs and scenarios describe applicability models. 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.

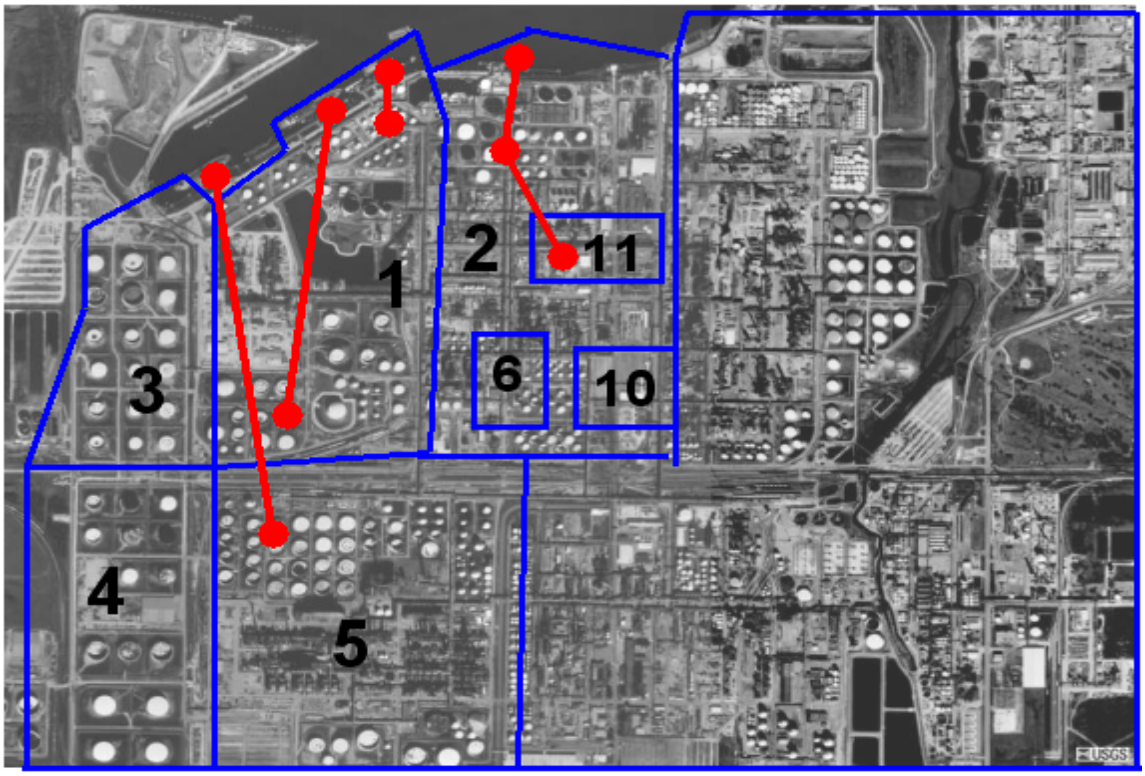
Regulatory Application Models

Image 1

Scenario (Image 1)	**Description**	**Regulated Area**
1	A Marine Transportation Related (MTR) facility transferring cargo through a pipeline that crosses a public street. However, the first valve within containment is located on the facility property across the street.	The facility is regulated by 33 CFR 105. The facility's security assessment will highlight how the properties are inter-related.
2	Same as above, except 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,

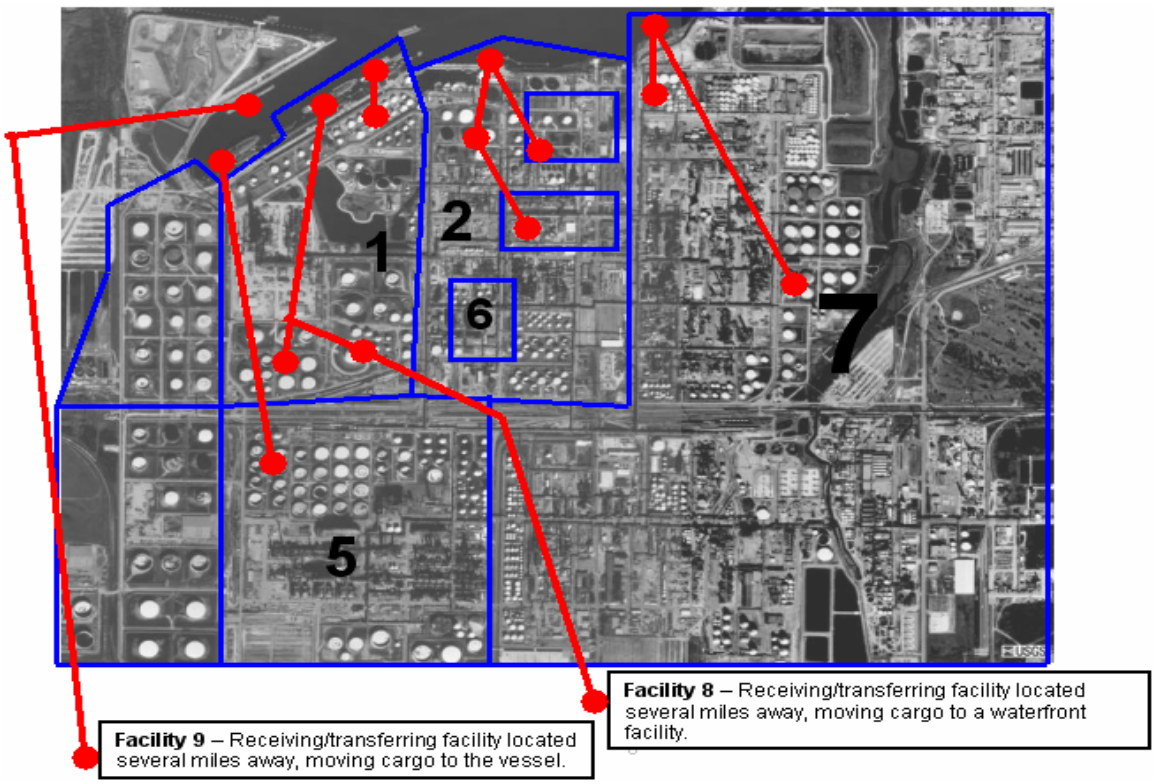
		then that facility on which the controls are located will be regulated by 33 CFR 105.

Image 2



Scenario (Image 2)	**Description**	**Regulated Area**
3	**Facility 1** is located along the waterfront transferring cargo to storage tanks located adjacent to the waterfront, and to tanks within the manufacturing facility that is 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 it could 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 this facility and has no marine activities. Facility 10 is located inside the facility and along the perimeter, but has its own entrance and exit separate from Facility 2. Facility 11 is located inside the perimeter of Facility 2, and transfers cargo to a 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. Facility 2's security plan should address security measure for Facility 6, 10, and 11 which is enclosed within the perimeter (i.e. access control, etc.)
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 would not be subject to the 33 CFR 105 requirements
6	**Facility 4** is located in an area near the waterfront, but is not on the waterfront and does not have any MTR activities.	**Facility 4** is not regulated by the Coast Guard, and would not be subject to the 33 CFR 105 requirements

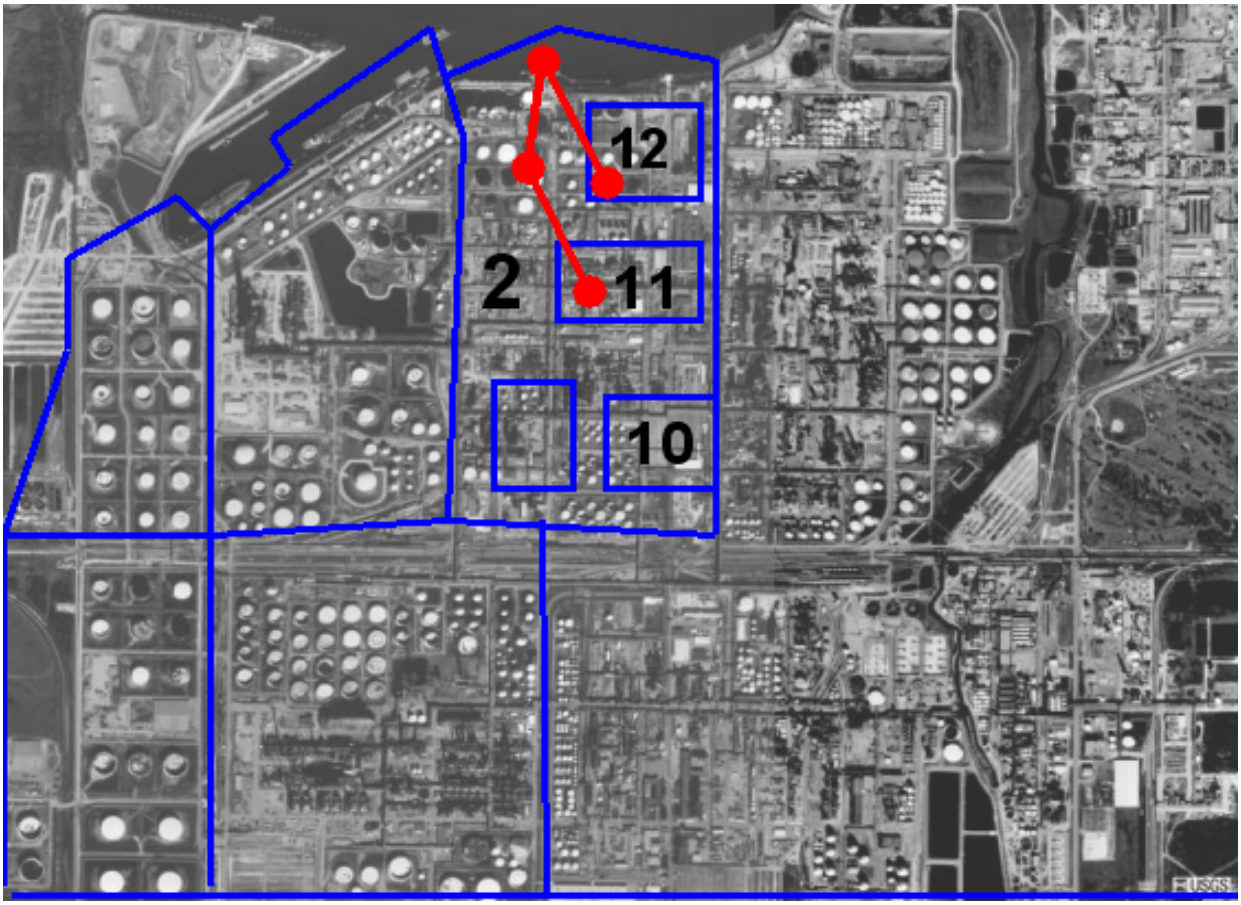
Image 3



Scenario (Image 3)	**Description**	**Regulated Area**
7	**Facility 5** is not located on the waterfront itself, but it does have a Marine Transportation Related (MTR) facility, which transfers product back into the storage tanks within the facility. The "first valve inside 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.
8	**Facility 6** is located inside Facility 2. Facility 6 does not have any Marine Transportation Related (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 of Facility 2. Facility 6 is not subject to 33 CFR 105.
9	**Facility 7** is a facility similar to Facility 1 located along the waterfront transferring 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	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.

	from Facility 1 that transfers cargo to the MTR facility.	
11	**Facility 9** transfers cargo through a pipeline to a production and storage facility located 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. If the production portion of the facility has control of the product in the pipeline, portions of that facility will need to be included in the plan.

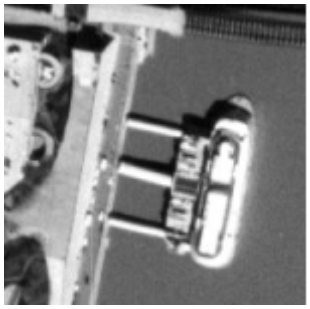
Image 4



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 does not have to be made to enter Facility 10.)	Facility 10 does not have to be in compliance with 33 CFR 105.
13	**Facility 11** is located within Facility 2, and personnel must pass through Facility 2's access control to enter Facility 11. Facility 11	Facility 11 will to be considered as part of the assessment of Facility 2. Facility 11 is not required to be in compliance with

	transfers cargo to a storage tank located within Facility 2, which transfers to/from vessels.	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. If Facility 2's facility security plan is not include Facility 12's vulnerability assessment and FSP, Facility 12 will have to develop its own security plan.

Image 5



Scenario (Image 5)	**Description**	**Regulated Area**
15	Facility in image 5 is a dock that has a Casino boat that is 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 CFR105.
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 return to the same facility to disembark the passengers.	The vessel and the facility are both required having 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 to 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 104/105. The plans may be consolidated. The plan will have to be submitted to both MSC (for vessels) and the local COTP (for the facilities). The plan will be cross-index for both vessels and facilities. This refers to ferries that are not involved in coastwise or international voyages.
18	(No image provided) Facility receives a vessel on ***international voyage*** carrying a non-hazardous material (i.e. rock, limestone, wood, timber, etc.) calls on a manned/unmanned facility. In many cases, the vessel conducts the transfer operation with no shore assistance.	The facility must be in compliance with 33 CFR 105 and develop a facility security plan.
19	(No image provided) The same as above but the vessels are only domestic	The facility only receives domestic route vessels and does not receive certain dangerous cargos (CDC's) and is not required to be in compliance with 33 CFR 105.

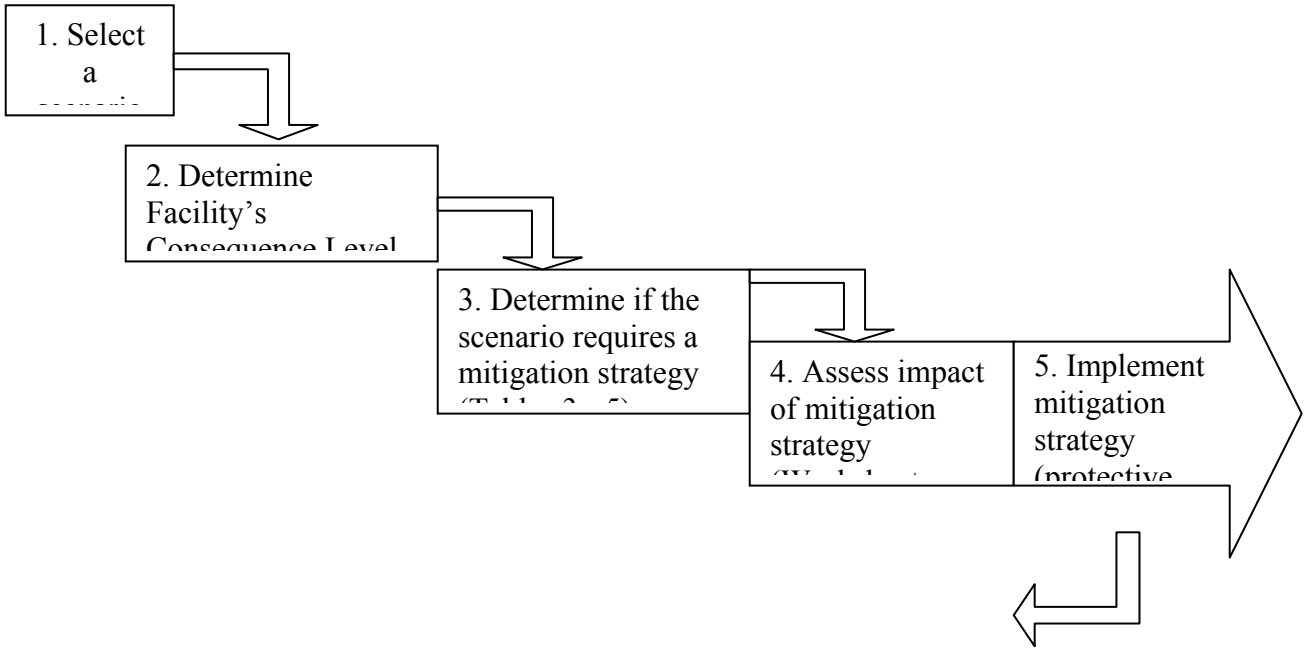
Guidance on Assessing Facility Security Measures

A security assessment performed in accordance with this enclosure may be used to evaluate the need for specific measures or evaluate alternate measures.

Risk-based decision-making is one of the best tools to perform a security assessment and to determine appropriate security measures for a facility. Risk-based decision-making is a systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual, or function and to identify actions that will reduce the vulnerability to and mitigate the consequences of a security breach.

A security assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach, and may suggest options to eliminate or mitigate those weaknesses. For example, a security assessment might reveal weaknesses in an organization's security systems or unprotected access points such as the facility's perimeter not being lighted or gates not being secured or monitored after hours. To mitigate this vulnerability, a facility would implement procedures to ensure that such access points are secured and verified by some means. Another security enhancement might be to place locking mechanisms and/or wire mesh on doors and windows that provide access to *restricted areas* to prevent unauthorized personnel from entering such spaces. Such assessments can identify vulnerabilities in facility operations, personnel security, and physical and technical security.

The following is a simplified risk-based security assessment, outlined in the following flow chart, which can be further refined and tailored to specific *facilities*. The process and results should be documented, (example provided in Table 5), when performing the assessment.



Note: Repeat process until all unique scenarios have been evaluated.

STEP 1: POTENTIAL THREATS

To begin an assessment, a facility or company needs to consider attack scenario(s) that consist of a potential threat to the facility under specific circumstances. It is important that the scenario or scenarios are within the realm of possibility and, at a minimum, address known capabilities and intents as given by a threat assessment. They should also be consistent with scenarios used to develop the Port Security Plan. For example, a bomb threat at a major petrochemical facility is one credible scenario. Table 1 provides a notional list of scenarios that may be combined with specific critical targets to develop the scenarios to be evaluated in the Facility Security Assessment.

The number of scenarios is left to the judgment of the facility or company. An initial evaluation should at least consider those scenarios provided in Table 1. Care should be taken to avoid unnecessarily evaluating an excessive number of scenarios that result in low consequences. Minor variations of the same scenario also do not need to be evaluated separately unless there are measurable differences in consequences.

Table 1: Notional List of Scenarios

Typical Types of Scenarios		**Application Example**
Intrude and/or take control of the target and ...	Damage/destroy the target with explosives	Intruder plants explosives.
	Damage/destroy the target through malicious operations/acts	Intruder takes control of a facility intentionally opens valves to release oil or hazmat that may then be ignited.
	Create a hazardous or pollution incident without destroying the target	Intruder opens valves/vents to release oil or toxic materials or releases toxic material brought along.
	Take hostages/kills people	Goal of the intruder is to kill people.
Externally attack the facility by …	Launching or shooting weapons from a distance	Shooting at a target using a rifle, missile, etc to damage or destroy bulk storage tanks, dangerous cargo, etc.
Use the facility as a means of transferring …	Materials, contraband, and/or cash into/out of the country	Facility is used as a conduit for *Transportation security incidents*
	People into/out of the country	

STEP 2: CONSEQUENCE ASSESSMENT

For this step a *Facility Security Officer* or company official should determine the appropriate consequence level (3, 2, or 1) determined from Table 2. The appropriate consequence level should be based on the "Description" of the facility (i.e., one that transfers, stores, or otherwise contains *certain dangerous cargoes* would have a "3" consequence level).

Table 2: Consequence Level

Consequence Level	Description
3	***Facilities* that transfer, store, or otherwise handle a *certain dangerous cargoes***
2	***Facilities* that** **(1) Are subject to 33 CFR Parts 126 and 154 (other than *certain dangerous cargoes*);** **(2) Receive vessel(s) that are certificated to carry more than 150 passengers (other than those required to comply with 33 CFR 128); or** **(3) Receive vessels on international voyages including vessels solely navigating the Great Lakes**
1	***Facilities*, other than those above.**

STEP 3: VULNERABILITY ASSESSMENT

Each scenario should be evaluated in terms of the facility's vulnerability to an attack. Four elements of vulnerability could be considered in the vulnerability score: availability, accessibility, organic security, and facility hardness, described as follows:

AVAILABILITY	The facility's presence and predictability as it relates to the ability to plan an attack.
ACCESSIBILITY	Accessibility of the facility to the attack scenario. This relates to physical and geographic barriers that deter the threat without organic security.
ORGANIC SECURITY	The ability of security personnel to deter the attack. It includes security plans, communication capabilities, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent the attack.

FACILITY HARDNESS	The ability of the facility to withstand the specific attack based on the complexity of facility design and material construction characteristics.

The *Facility Security Officer* or company official should discuss each vulnerability element for a given scenario. The initial evaluation of vulnerability should be viewed with only existing strategies and protective measures, designed to lessen vulnerabilities, which are already in place. After the initial evaluation has been performed, a comparison evaluation can be made with new strategies and protective measures considered. Assessing the vulnerability with only the existing strategies and protective measures will provide a better understanding of the overall risk associated with the scenario and how new strategies and protective measures will mitigate the risk.

With the understanding that the facility has the greatest control over the accessibility and organic security elements, this tool only takes into consideration these elements (not addressing availability or facility hardness) in assessing each scenario. The vulnerability score and criteria with benchmark examples are provided in the following table. Each scenario should be evaluated to get an accessibility and organic security score. Then sum these elements to get the total vulnerability score (step 3 in Table 5). This score should be used as the vulnerability score when evaluating each scenario in the next step.

Table 3: Vulnerability Score

Score	Accessibility	Organic Security
3	No deterrence (e.g. unrestricted access to facility and unrestricted internal movement)	No deterrence capability (e.g. no plan, no guard force, no emergency communication, outside law enforcement not available for timely prevention, no detection capability
2	Fair deterrence (e.g. single substantial barrier; unrestricted access to within 100 yards of bulk storage tanks)	Fair deterrence capability (e.g. minimal security plan, some communications, security force of limited size relative to the facility; outside law enforcement with limited availability for timely prevention, limited detection systems)
1	Good deterrence (expected to deter attack; access restricted to within 500 yards of bulk storage tanks; multiple physical/geographical barriers)	Good deterrence capability expected to deter attack (e.g., detailed security plan, effective emergency communications, well trained and equipped security personnel; multiple detection systems [camera, x-ray, etc.], timely outside law enforcement for prevention).

STEP 4: MITIGATION

The facility or company should next determine which scenarios should have mitigation strategies (protective measures) implemented. This is accomplished by determining where the scenario falls in Table 4 based on the consequence level and vulnerability assessment score. Table 4 is intended as a broad, relative tool to assist in the

development of the *Facility Security Plan*. "Results" are not intended to be the sole basis to trigger or waive the need for specific measures, but are one tool in identifying potential vulnerabilities and evaluating prospective methods to address them.

The following terms are used in Table 4 as mitigation categories:

"Mitigate" means that mitigation strategies, such as security protective measures and/or procedures, should be developed to reduce risk for that scenario. An appendix to the *Facility Security Plan* should contain the scenario(s) evaluated, the results of the evaluation, and the mitigation measures chosen.

"Consider," means that mitigation strategies should be developed on a case-by-case basis. The *Facility Security Plan* should contain the scenario(s) evaluated, the results of the evaluation, and the reasons mitigation measures were or were not chosen.

"Document" means that the scenario may not need a mitigation measure and therefore needs only to be documented. However, measures having little cost may still merit consideration. The security plan should contain the scenario evaluated and the results of the evaluation. This will be beneficial in further revisions of the security plan, in order to know if the underlying assumptions have changed since the last security assessment.

Table 4: Vulnerability & Consequence Matrix

		Total Vulnerability Score (Table 3)		
		2	**3-4**	**5-6**
Level (Table 2)	3	**Consider**	**Mitigate**	**Mitigate**
	2	**Document**	**Consider**	**Mitigate**
	1	**Document**	**Document**	**Consider**

STEP 5: IMPLEMENTATION METHODS

To determine which scenarios require mitigation methods, the *Facility Security Officer* or company official may find it beneficial to use the Table 5 provided below. The facility or company can record the scenarios considered, the consequence level (Table 2), the score for each element of vulnerability (Table 3), the total vulnerability score, and the mitigation category (Table 4). The desire is to reduce the overall risk associated with the identified scenario. Note that generally, it is easier to reduce vulnerabilities than to reduce consequences or threats.

Table 5

MITIGATION DETERMINATION WORKSHEET					
Step 1	**Step 2**	**Step 3**			**Step 4**
Scenario/Description	**Consequence Level (Table 2)**	**Vulnerability Score (Table 3)**			**Mitigate, Consider, or Document (Table 4)**
		Accessibility +	Organic Security =	Total Score	
	Once a facility is categorized, the consequence level remains the same.				

To assist the *Facility Security Officer* or company official evaluate specific mitigation strategies (protective measures), it may be beneficial to use Table 6 provided below.

Table 6

MITIGATION IMPLEMENTATION WORKSHEET						
1	**2**	**3**	**4**			**5**
Mitigation Strategy (Protective Measure)	**Scenario(s) that are affected by Mitigation Strategy (from Step 1 in Table 5)**	**Consequence Level (Table 2)**	**New Vulnerability Score (Table 3)**			**New Mitigation Results (Table 4)**
			Accessibility +	Organic Security =	Total Score	
1.	1.					
	2.					
	…					
2.	…					

The following steps correspond to each column in Table 6.

1. For those scenarios that scored as **consider** or **mitigate**, the facility or company should brainstorm mitigation strategies (protective measures) and record them in the first column of Table 6.

2. Using the scenario(s) from Table 5, list all of the scenario(s) that would be affected by the selected mitigation strategy.
3. The consequence level remains the same as was determined in Table 2 for each scenario.
4. Re-evaluate the accessibility and organic security scores (Table 3) to see if the new mitigation strategy reduces the total vulnerability score for each scenario.
5. With the consequence level and new total vulnerability score, use Table 4 to determine the new mitigation categories.

A strategy may be deemed as effective if its implementation lowers the mitigation category (e.g. from **mitigate** to **consider** in Table 4). A strategy may be deemed as effective if the strategy will lower the overall vulnerability score when implemented by itself or with one or more other strategies. For example, for a facility with a consequence level of "2", if a mitigation strategy lowers the vulnerability score from "5-6" to "3-4", the mitigation category changes from **mitigate** to **consider** and the mitigation strategy is effective. For a facility with a consequence level of "3", the mitigation category would remain the same **(mitigate)** for a similar reduction in vulnerability score from "5-6" to "3-4".

It should be noted that if a mitigation strategy, when considered individually, does not reduce the vulnerability, then multiple strategies may be considered in combination. Considering mitigation strategies as a whole may reduce the vulnerability to an acceptable level.

As an example of a possible vulnerability mitigation measure, a facility or company may contract for additional security personnel to prevent unauthorized access during times of elevated threat levels. This measure would improve physical security and may reduce the total vulnerability score from a "3-4" to a "2". However this option is specific for this scenario and also carries a certain cost.

A strategy may be deemed feasible if it can be implemented with little operational impact or funding relative to the prospective reduction in vulnerability. A strategy may be deemed partially feasible if its implementation requires significant changes or funding relative to the prospective reduction in vulnerability. A strategy may be deemed not feasible if its implementation is extremely problematic or is cost prohibitive.

Feasibility of a mitigation strategy may vary based on the *MARSEC level*. Therefore, some strategies may not be warranted at *MARSEC Level 1*, but may be at *MARSEC Levels 2* or *3*. For example, using divers to inspect the underwater pier structures and vessel may not be necessary at *MARSEC Level 1*, but may be appropriate if there is a specific threat and/or an increase in *MARSEC level*. Mitigation strategies should ensure that the overall level of risk to the facility remains constant relative to the increase in threat.

Tables 7 and 8 provide an abbreviated example of how Tables 5 and 6 would be filled out for a bulk oil facility that is subject to 33 CFR 154 and receives vessels on international voyages. This example assumes that the facility has a fair deterrence capability with respect to organic security, however does not have a fenced perimeter to restrict access to the facility.

Table 7

MITIGATION DETERMINATION WORKSHEET					
Step 1	**Step 2**	**Step 3**			**Step 4**
Scenario/Description	**Consequence Level (Table 2)**	**Vulnerability Score (Table 3)** **Accessibility + Organic = Total Security Score**			**Mitigate, Consider, or Document (Table 4)**
1. Gain unauthorized entry into the facility.	**2**	**3**	**2**	**5**	**Mitigate**
2. Externally attack the facility with a firearm.		**3**	**2**	**5**	**Mitigate**
3. Use the facility as a means of transferring people from a ship to a vehicle to illegally enter the U.S.		**3**	**2**	**5**	**Mitigate**
…		**…**	**…**	**…**	**…**

Table 8

MITIGATION IMPLEMENTATION WORKSHEET						
1	**2**	**3**	**4**			**5**
Mitigation Strategy (Protective Measure)	**Scenario(s) that are affected by Mitigation Strategy (from Step 1 in Table 5)**	**Consequence Level (Table 2)**	**New Vulnerability Score (Table 3)** Accessibility +	Organic =	Total Score	**New Mitigation Results (Table 4)**
1. Perimeter Fence that Restricts Access to the facility (meeting ASIS standards)	1. Intrude to the facility.	**2**	**2**	**2**	**4**	**Consider**
	2. Use the facility as a means of transferring people from a ship to a vehicle to illegally enter the U.S.		**2**	**2**	**4**	**Consider**
	…		…	…	…	…
2…	…		…	…	…	…