U.S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-MOC
Phone: (202) 267-0493
Fax: (202) 267-4394
Email: fldr-g-moc@comdt.uscg.mil

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

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

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

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

2. ACTION.

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

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

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

DISTRIBUTION – SDL No. 141

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

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

5. DISCUSSION.

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

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

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

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

6. IMPLEMENTATION.

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

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

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

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

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

7. INFORMATION SECURITY.

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

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

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

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

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

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

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

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

U.S. Department of Homeland Security

United States Coast Guard

Unit

Address
Staff Symbol:
Phone:
Fax:

SSIC
Date
MISLE Activity # XXXXXXX
FIN #: XXXXXX

Company Name
Address
City, State, Zip

SAMPLE LETTER OF AUTHORIZATION

Dear Mr./Ms. XXXX:

The Facility Security Plan (FSP) for *[Facility Name]*, submitted to meet the requirements of Title 33 Code of Federal Regulations (CFR) Part 105, is currently under review by the U.S. Coast Guard. *[Facility Name]* may continue to operate in accordance with all the provisions of the submitted plan pending final determination of FSP approval. This Letter of Authorization will expire on *[NLT October 31, 2004]*, at which time the Coast Guard will reevaluate the status and progress of your plan submission.

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

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

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

Sincerely,

Captain of the Port or
Designated representative

U.S. Department of Homeland Security

United States Coast Guard

Unit

Address
Staff Symbol:
Phone:
Fax:

SSIC
Date
MISLE Activity # XXXXXXX
FIN #: XXXXXXX

Company Name
Address
City, State, Zip

SAMPLE INTERIM APPROVAL LETTER

Dear Mr./Ms. XXXX:

The facility security plan for *[Facility Name]*, submitted to meet the requirements of Title 33 Code of Federal Regulations (CFR) Part 105, is approved on an interim basis. This Interim Letter of Approval will expire on *[NLT October 31, 2004]*, at which time the Coast Guard will reevaluate the status and progress of your plan submission. Your facility shall continue to work proactively with the National FSP Review Center to correct any remaining deficiencies with your security plan.

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

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

Sincerely,

Captain of the Port or
Designated representative

ENCLOSURE 10
MTSA FACILITY COMPLIANCE GUIDE

Use of the MTSA Facility Compliance Guide

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

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

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

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

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

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

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

United States Coast Guard

MTSA FACILITY COMPLAINCE GUIDE

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

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

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

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

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

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

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

FIN # _____

Insp Initials _____
Date _____

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

FIN # _____

Insp Initials _____
Date _____

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

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

FIN # _____

Insp Initials _____
Date _____

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

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

FIN # _____ Insp Initials _____
Date _____

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

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

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

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

FIN # _____ Page 8 of 14 Insp Initials _____

Date _____

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

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

- Section continued on next page -

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

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

FIN # _____

Insp Initials _____
Date _____

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

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

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

FIN # _____ Page 11 of 14 Insp Initials _____
Date _____

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

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

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

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

--- Notes on deficiencies ---

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

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

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

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

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

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

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

Inspection Summary

Comments:

ENCLOSURE 11
ADDITIONAL POLICY GUIDANCE

11.1. Enclosure Contents

11.1.1. This enclosure contains the following additional policy guidance:

11.2 Introduction
11.3 Plan Submission
11.4 Compliance Documentation
11.5 Alternative Security Programs (ASP)
11.6 Temporary Equivalent Security Measures
11.7 FSP Letter of Approval
11.8 Interim Letter of Approval (ILA)
11.9 Letter of Authorization to Operate (LOA)
11.10 Non-Compliant Facilities
11.11 Enforcement Philosophy
11.12 Enforcement Cycle and Control Actions
11.13 Additional Compliance Checks for Facilities Receiving Vessels Subject to SOLAS Chapter XI-2 and ISPS
11.14 Suspending Operations
11.15 Intermittent Operations
11.16 Lower Consequence Plan Review Methodology

Policy Advisory Council Decisions
11.17 Declaration of Security (DoS) Applicability
11.18 Facilities with Megayachts
11.19 Remote Facilities
11.20 Facilities Handling Cargoes Regulated by 46 CFR Part 148
11.21 Facilities that Receive Drilling Mud
11.22 Checking Identification and Performing Passenger, Baggage, Vehicle Screening
Addendum (1) Decision Tool for issuing Letters of Approval, Interim Letters of Approval, and Letters of Authorization
Addendum (2) Declaration of Security (DoS) Applicability Decision Tool
Addendum (3) MTSA Compliance Matrix
Addendum (4) MTSA Compliance Guide (Internal CG Use Only)

11.2 Introduction

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

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

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

11.3 Plan Submission

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

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

11.4. Compliance documentation

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

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

11.5 Alternative Security Programs (ASP)

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

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

11.6 Temporary equivalent security measures

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

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

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

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

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

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

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

11.7 FSP Letter of Approval

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

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

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

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

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

11.8 Interim Letter of Approval (ILA)

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

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

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

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

11.9 Letter of Authorization (LOA)

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

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

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

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

11.10 Non-Compliant Facilities

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

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

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

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

11.11 Enforcement Philosophy

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

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

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

11.12. Enforcement Cycle and Control Actions

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

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

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

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

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

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

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

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

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

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

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

11.14 Suspending Operations

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

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

11.15 Intermittent Operations

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

11.16 Lower Consequence Plan Review Methodology

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

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

11.17 Declaration of Security (DoS) Applicability

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

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

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

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

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

11.18 Facilities with Megayachts

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

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

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

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

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

11.19 Remote Facilities

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

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

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

11.20 Facilities Handling Cargoes Regulated by 46 CFR Part 148

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

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

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

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

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

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

11.21 Facilities that receive drilling mud

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

11.22 Checking Identification and Performing Passenger, Baggage, Vehicle Screening

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

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

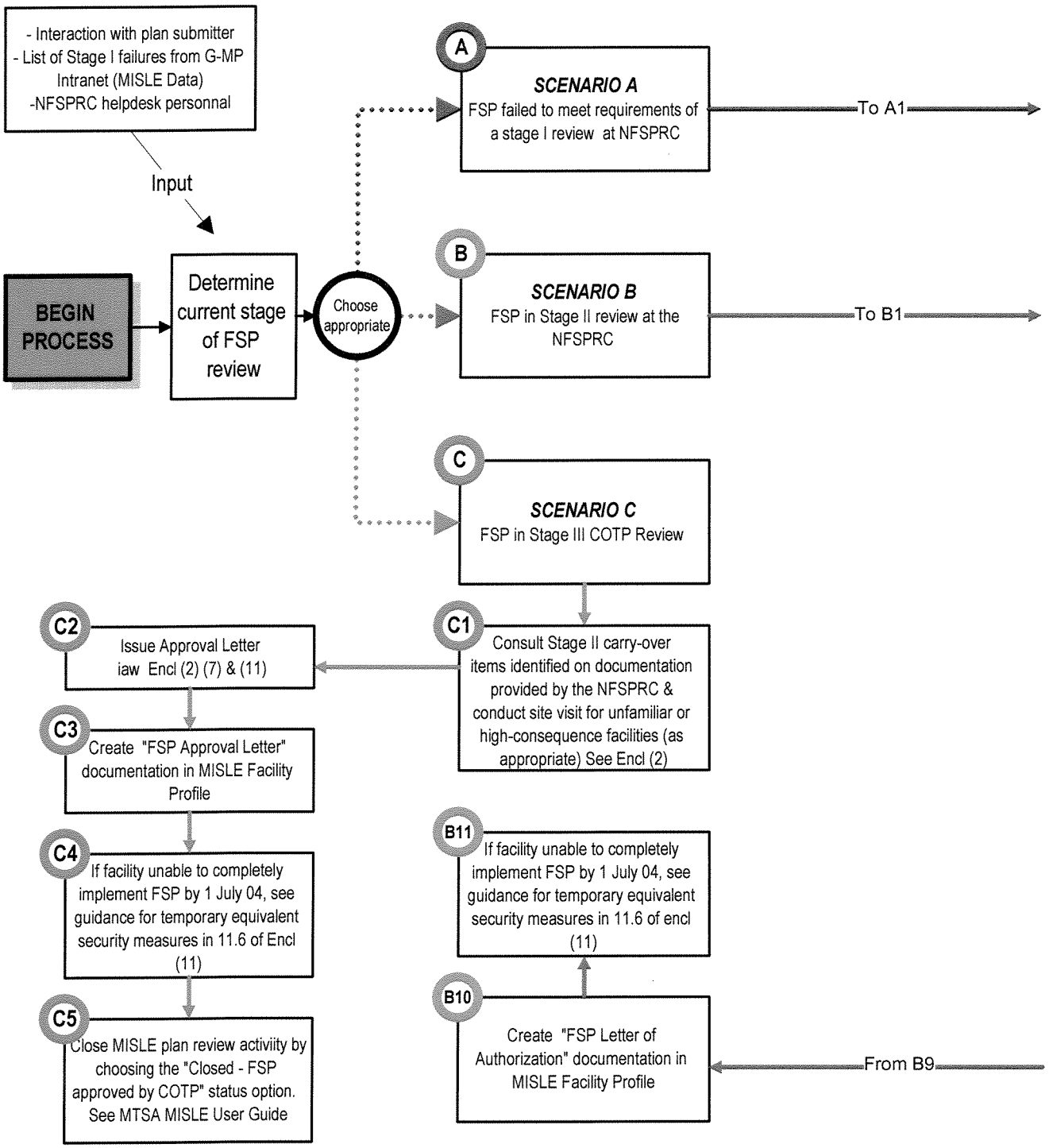
11.22.3. At this time there is no alternative for vehicle screening. All facilities must screen vehicles at the rate specified in the applicable MARSEC Directive.

ADDENDUM (1) to ENCLOSURE (11)

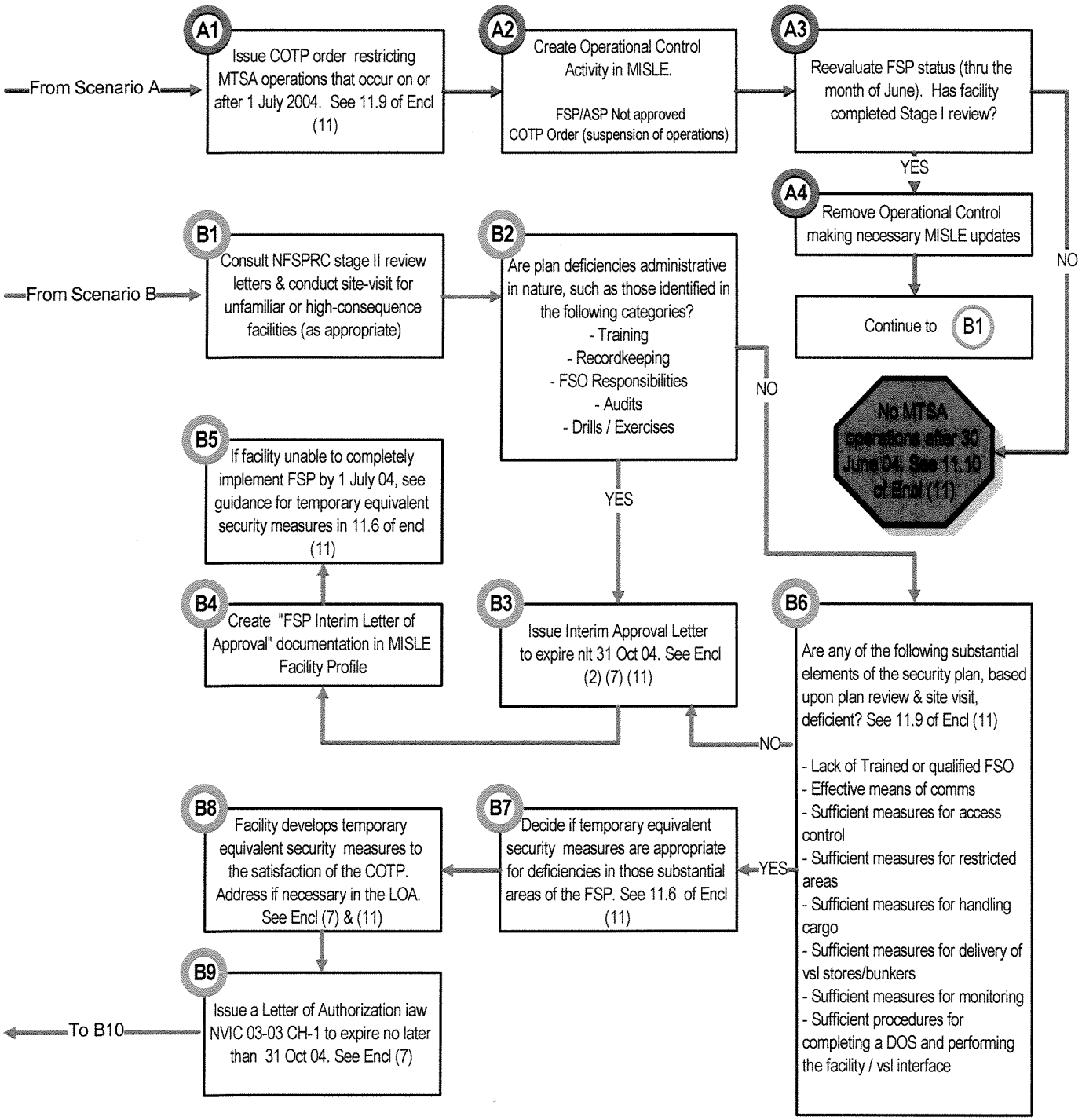
Decision Tool for issuing Letters of Approval, Interim Letters of Approval, and Letters of Authorization

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

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



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



ADDENDUM (2) to ENCLOSURE (11)

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

DECLARATION OF SECURITY (DoS) APPLICABILITY DECISION TOOL

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

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

TABLE 1 - VESSEL / FACILITY CATEGORY DECISION MATRIX

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

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

TABLE 2 – DOS INTERFACE DECISION MATRIX

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

Table Legend

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

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

ADDENDUM (3) to ENCLOSURE (11)

MTSA Compliance Matrix

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

CODES FOR CONTROL & COMPLIANCE MEASURES

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

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

CODES FOR PENALTY MEASURES

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