U.S. Department of Homeland Security

United States Coast Guard

Commandant
United States Coast Guard

2100 2nd ST SW
Washington DC 20593-0001
Staff Symbol: (CG-544)
Phone: (202) 372-1000

COMDTPUB P16700.4
NVIC 03-03 Change 2

FEB 28 2009

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 03-03, Change 2

Subj: CH-2 to 03-03, IMPLEMENTATION GUIDANCE FOR THE REGULATIONS MANDATED BY THE MARITIME TRANSPORTATION SECURITY ACT OF 2002 (MTSA) FOR FACILITIES

Ref:
(a) Title 33 Code of Federal Regulation, Part 101
(b) Title 33 Code of Federal Regulation, Part 105
(c) International Ship & Port Facility Security (ISPS) Code
(d) Title 49 Code of Federal Regulation, Part 1520
(e) Navigation and Vessel Inspection Circular NO. 03-07
(f) Navigation and Vessel Inspection Circular NO. 10-04
(g) 46 USC 70103
(h) 46 USC 70119
(i) Safe Port Act Message of 07 JUL 2007
(j) Maritime Transportation Security Act Facilities and the Chemical Facility Anti-Terrorism Standards (CFATS) Message – R261428 Dec 07
(k) Maritime Security Risk Assessment Model (MSRAM)

1. PURPOSE. This document revises Navigation and Vessel Inspection Circular (NVIC) No. 03-03, Change 1. It is designed to provide further clarity and guidance for the implementation of the maritime security regulations mandated by the Maritime Transportation Security Act of 2002 (MTSA). This document also introduces the process of submitting security plans and security plan amendments by way of HOMEPORT, information regarding the new Transportation Worker Identification Credential (TWIC) rule and its applicability to regulated facilities and requirements of the Safe Port Act including scheduled and non-scheduled facility inspections.

DISTRIBUTION – SDL No. 150

	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																									25	
D	1	2		1	1						1															
E														2												
F					1					1																
G																										
H																										

This NVIC details Facility Security Plan implementation, the plan review process, provides guidance to successfully execute compliance inspections, adds information for guidance for the purposes of performing Facility Security Assessments, and provides clarification on the applicability of MTSA mandated regulations found in 33 CFR part 105.

2. ACTION. 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 through HOMEPORT at http://homeport.uscg.mil.

   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 and to examine the process of submitting facility security plan documents by way of HOMEPORT. It is also an aid to Coast Guard personnel and facility owner/operators in gaining the necessary information for the successful implementation of TWIC.

3. DIRECTIVES AFFECTED. NVIC 03-03, Change 1 is superseded. Change 2 provides additional clarity and guidance on the Final Rules on Maritime Security, 33 CFR Subchapter H, and the Maritime Transportation Security Act (MTSA) of 2002. Enclosures (1) & (2) were combined by placing the Plan Review Guidance Flowchart into Enclosure (2) and renaming it as Enclosure (1). An additional flowchart was added illustrating the use of HOMEPORT for the submission of FSPs. Enclosures (3) and (4b) were removed to reflect the elimination of Stage 1 & Stage 2 reviews of Facility Security Plans. Enclosure (7) was updated to include the TWIC program, Safe Port Act 2006 requirements, and areas of emphasis for security spot checks. Enclosure (8) was added to provide guidance for those who perform security audits. Enclosure (10) was added regarding training standards of explosive dog teams. The remainder of NVIC 03-03 is unchanged. Enclosure (11) was added to provide guidance for those who perform only security spot checks.

4. BACKGROUND. NVIC 03-03, Change 1 was published to assist COTP personnel as well as owners and operators of affected facilities in complying with the maritime security regulations in MTSA. Change 2 makes available information regarding ongoing amendments and clarifications in the implementation of the requirements found in 33 CFR 105, as a result of the mandates from Safe Port Act.

5. DISCUSSION. Captain of the Port (COTP) personnel will conduct examinations of affected facilities to determine compliance with 33 CFR 105 and their approval. Enclosure (7) MTSA Facility Compliance Guide and Enclosure (8) Facility Security Audits, provide detailed guidance for facility inspectors and outline specific performance criteria based on the regulatory requirements of 33 CFR 105. Once completed, examination checklists shall be treated as Sensitive Security Information (SSI) and handled accordingly.

   Enclosure (8), Facility Security Audits, was added to provide more in depth information for both facility owner/operators and Coast Guard personnel regarding annual security audits. This enclosure describes the intent of the regulation and the purpose of performing an annual audit. It provides guidance for the process of performing and evaluating annual security audits. Included is a sample audit report form which may be used by an auditor to assist in the preparation and documentation of audit findings

As additional guidance and clarifications continue to be developed, the HOMEPORT website http://homeport.uscg.mil should be regularly consulted for the most up-to-date policy guidance and information.

MTSA regulations do not mandate specific equipment or procedures, but call for performance-based criteria to ensure the security measures are satisfactorily implemented at a facility. The MTSA Facility Compliance Guide, Enclosure (7), is designed to assess not only the facilities compliance with their approved FSP, but the adequacy of the FSP in addressing the performance criteria outlined in the regulations.

6. INFORMATION SECURITY. 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 the handling of SSI materials 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 49 CFR 1520 for the marking, storing, distributing, and destroying of SSI materials, which includes many documents that discuss screening processes and detection procedures.

   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 have a need to know the provisions of the security plans and assessments and restrict dissemination of these documents accordingly. To ensure that access is restricted only to authorized personnel, SSI material will not be disclosed under the Freedom of Information Act (FOIA) for most circumstances.

   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.

7. DISCLAIMER. While the guidance contained in this document may assist the industry, the public, the Coast Guard, and other Federal and State agencies responsible for enforcing statutory and regulatory requirements, the guidance is not a substitute for applicable legal requirements, nor is it 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.

8. CHANGES. This NVIC will be posted on the HOMEPORT at http://homeport.uscg.mil. 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 in the next change to this circular.

9. ENVIRONMENTAL ASPECT AND IMPACT CONSIDERATION. Environmental considerations were examined in the development of this manual and have been determined to be not applicable

10. FORMS/REPORTS. None.

JAMES A. WATSON
Rear Admiral, U.S. Coast Guard
Director of Prevention Policy

Encl: Navigation and Vessel Inspection Circular No. 03-03, Change 2

IMPLEMENTATION GUIDANCE FOR THE REGULATIONS MANDATED BY THE MARITIME TRANSPORTATION SECURITY ACT OF 2002 (MTSA) FOR FACILITIES

TABLE OF CONTENTS

Enclosure (1) – MTSA Facility Security Plan (FSP) Implementation Process Methodology

1.1 Enclosure Contents 1-1
1.2 Facility Security Plan (FSP) Review Process – General 1-1
1.3 FSP Submissions 1-1
1.4 Review of FSPs 1-1
1.5 COTP Review and Approval of FSPs 1-2
1.6 Implementation of Inspection Cycles 1-3
1.7 Enforcement Strategies – Plan Submission 1-3

Addendum (1) – FSP, Submission, Review Approval, Denial Chart 1-5
Addendum (2) – Homeport FSP Submission, Review, Approval, Denial Chart 1-6
Addendum (3) – Examples of Major and Minor Deficiencies 1-7

Enclosure (2) – General Guidance for FSP Preparers and Reviewers

2.1 Security Administration and Organization of the Facility 2-1
2.2 Personnel Training 2-1
2.3 Drills and Exercises 2-1
2.4 Records and Documentation 2-1
2.5 Response to Change in MARSEC Level 2-1
2.6 Communications 2-1
2.7 Procedures for Interfacing with Vessels 2-1
2.8 Declaration of Security (DoS) 2-1
2.9 Security Systems and Equipment Maintenance 2-1
2.10 Security Measures for Access Control, including designated public access areas 2-2
2.11 Security Measures for Restricted Areas 2-2
2.12 Security Measures for Handling Cargo 2-2
2.13 Security Measures for Delivery of Vessel Stores and Bunkers 2-2
2.14 Security Measures for Monitoring 2-2
2.15 Security Incident Procedures 2-2
2.16 Audit and Security Plan Amendments 2-2

2.17 Facility Security Assessment (FSA) Report 2-2
2.18 Facility Vulnerability and Security Measures Summary (Form CG-6025) 2-3
2.19 Additional Requirements for Passenger and Ferry Facilities 2-3
2.20 Additional Requirements for Cruise Ship Terminals..... 2-3
2.21 Additional Requirements for CDC Facilities..... 2-3
2.22 Additional Requirements for Barge Fleeting Facilities 2-3

Enclosure (3) – FSP Review Checklist for Preparers and Reviewers 3-1
Enclosure (4) – Sample Plan Review-Related Letters 4-1
Enclosure (5) – Additional Applicability Guidance 5-1
Enclosure (6) – Sample Declaration of Security (DOS) 6-1
Enclosure (7) – MTSA Facility Compliance Guide 7-1
Enclosure (8) – Facility Security Audits 8-1
Enclosure (9) – Guidance for Submission of Alternative Security Programs, Equivalency and Waiver Requests 9-1
Enclosure (10) – Guidance for Training, Standards, and Auditing of Explosive Detection Dog Teams 10-1
Enclosure (11) – USCG Facility Security Spot Check Guide 11-1

ENCLOSURE 1

MTSA FSP IMPLEMENTATION PROCESS METHODOLOGY

1.1 Enclosure Contents

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

1.2 Facility Security Plan (FSP) Review – General
1.3 FSP Submissions
1.4 Review of FSPs
1.5 COTP Review and Approval of FSPs
1.6 Implementation of Inspection Cycles
1.7 Enforcement Strategies – Plan Submission
Addendum (1) Facility Security Plan (FSP) Submission, Review, Approval / Denial Flow Chart
Addendum (2) Homeport Submission Flow Chart
Addendum (3) Examples of Major and Minor Deficiencies

1.2 Facility Security Plan (FSP) Review Process - General

1.2.1 The plan review process is critical to the successful implementation of MTSA regulations. The following is a brief discussion of each critical aspect of this process. A flow-chart of this process is contained in this section as Addendum (1). An on-site verification may be necessary, depending on the familiarity of the plan reviewer with the specific facility. Facilities must comply with their security plan while conducting regulated operations or risk enforcement actions which may include suspension of operations until compliance is reached.

1.3 FSP Submissions

1.3.1 All facilities subject to 33 CFR 105 must submit FSPs to the cognizant COTP in accordance with 33 CFR 105.310, 33 CFR 105.410 and, if applicable, HOMEPORT guidance provided in Addendum (2).

1.3.2 Upon receipt, the COTP shall date stamp the FSP submittal.

1.3.3 Review personnel will screen all plans upon receipt to determine applicability to 33 CFR Part 105 and will review only those as required by that part. Review personnel **will** consult with the COTP before determining whether or not regulations apply to a specific submission and prior to returning the plan to the submitter. Enclosure (5) provides additional guidance toward defining an individual facility's regulated areas.

1.4 Review of FSPs

1.4.1 Following a successful applicability screening, plans undergo an initial review to ensure the eighteen basic required sections are properly included/addressed. Review personnel will utilize the review form incorporated as Enclosure (3) Sections A and B. Major deficiencies noted during the review will require the plan to be resubmitted with corrections prior to further review. Major deficiencies include the following:

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

1.4.2 Plans will then be screened to determine whether they were submitted in accordance with 33 CFR 105.410. All plans will be reviewed in the order received.

1.4.3 In the case that a Facility Identification Number (FIN) does not exist, one will be assigned by the reviewer. Following a successful "applicability" determination, review personnel will create a Plan Review Sub-Activity within MISLE. MISLE information will be audited to ensure database integrity through a review of the FIN and PARTICULARS tables maintained by CG-382.

1.4.4 After the successful completion of MISLE activities, a letter will be mailed to the plan owner from the COTP containing:

- A statement acknowledging receipt of their plan;
- The unique Activity Number for their plan review activities; and
- Plan reviewer contact information.

1.4.5 The comprehensive review assesses the plan's compliance with all regulatory requirements contained in 33 CFR 105. The review form is incorporated as Enclosure (3) Section C.

1.4.6 To expedite reviews, plans will not be returned for minor corrections. Instead, plan owners may receive a letter from or be contacted directly by review personnel identifying minor deficiencies and the timeframe for submitting revisions.

1.5 COTP Review and Approval of FSPs

1.5.1 Following a successful review, the FSP will be presented to the cognizant COTP for final review and approval. The COTP will also receive copies of:

- FSA report,
- Review notes,
- All correspondence between the plan submitter and review personnel, and
- A summary detailing any review form items that could not be accurately verified by review personnel.

1.5.2 The final review verifies the FSA information against the physical characteristics of the entire facility. (See guidance in Enclosure 5.)

1.5.3 The COTP will determine whether to approve or not approve the Facility Security Plan (FSP) taking into consideration information contained in the Area Maritime Security Plan (AMSP), the Maritime Risk Assessment Model (MSRAM) data and the FSP under review.

1.5.4 If major deficiencies are identified during the review process, the COTP may:

- Return the plan to review personnel for further action detailing deficiencies found, or
- Deny approval of the FSP and return the FSP to the submitter with a letter noting deficiencies and timeframe for resubmitting the FSP.

Major deficiencies are those that cannot be easily corrected by the plan owner in a timely manner, or that would require significant changes or alterations to the plan requiring additional review.

1.5.5 Following a successful review, the COTP shall issue an FSP Letter of Approval. The plan review process is now complete. A sample plan approval letter is contained in Enclosure (4). The COTP closes the MISLE Plan Review Sub-Activity and files the plan in a secure location, in accordance with Sensitive Security Information (SSI) protocols.

1.6 Implementation of Inspection Cycles

1.6.1 Coast Guard personnel will enforce and verify the facility is implementing security measures contained in their FSP when conducting annual compliance examinations or security spot check checks. These inspections may also include verifying compliance with the following regulatory requirements (as applicable):

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

1.6.2 Captain of the Ports (COTPs) will utilize a risk-based approach to determine priorities when scheduling compliance inspections. COTPs are expected to schedule these compliance inspections taking into account all of the following tools/criteria:

- Maritime Security Risk Assessment Model (MSRAM);
- Facility inspection history (past deficiencies/violations);
- Facility inspection cycle/schedule;
- Economy of personnel resources.

1.7 Enforcement Strategies – Plan Submission

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

1.7.2 33 CFR 105.410(b) states that owners or operators of facilities not in service on or before 31 December 2003 must comply with the requirements of 33 CFR 105.410(a) 60 days prior to beginning operations.

1.7.3 33 CFR 101.415, as amended, allows for civil penalties 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:

- Restrictions on facility access;
- Conditions on facility operations;
- Suspension of facility operations;
- Lesser administrative and corrective measures; or
- Suspension or revocation of security plan approval, thereby making that facility ineligible to operate.

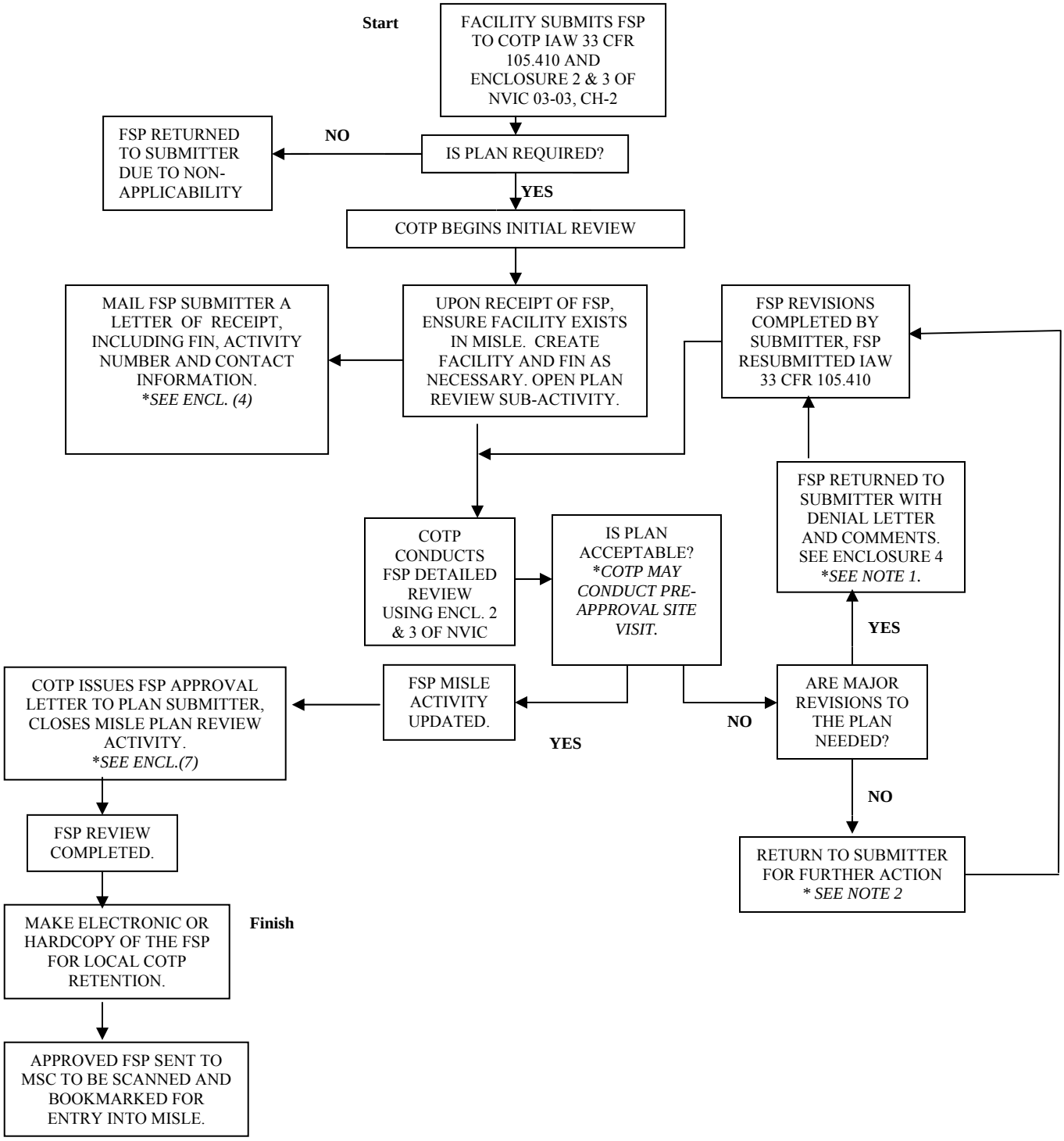
1.7.4 The COTP will note that the Facility Security Assessment Report and the Facility Vulnerability and Security Measures Summary (Form CG-6025) are critical in summarizing a facility's vulnerabilities and the security measures used to mitigate them. COTPs will use this information to aid in the revision and updating of Area Maritime Security Plans and to audit FSP implementation. Facility owners are strongly encouraged to complete the CG-6025 with a focus on the highest-risk and consequence vulnerabilities by using the nine vulnerability categories listed in the Key to the Form. Facility owners/operators should complete this form for each of these nine vulnerability categories. If there is more than one vulnerability issue under the same category, list them. However, the list should focus on approximately three of the most important entries for the category, and identifying all vulnerabilities that may be exploited to cause a Transportation Security Incident (TSI) as defined in 33 CFR 101.105.

Facility owner/operators are encouraged to submit and administer their FSP by utilizing Homeport (see Addendum 2). In such cases the administration, submission, review, and approval/denial of the FSP will proceed in accordance with the protocol(s) governing the use of Homeport. Homeport will mirror the process sequencing described in Addendum (1).

MISLE entries will be made in accordance with protocols governing the use of MISLE.

Facility Security Plan (FSP)

SUBMISSION, REVIEW, APPROVAL OR DENIAL (Non-Homeport)

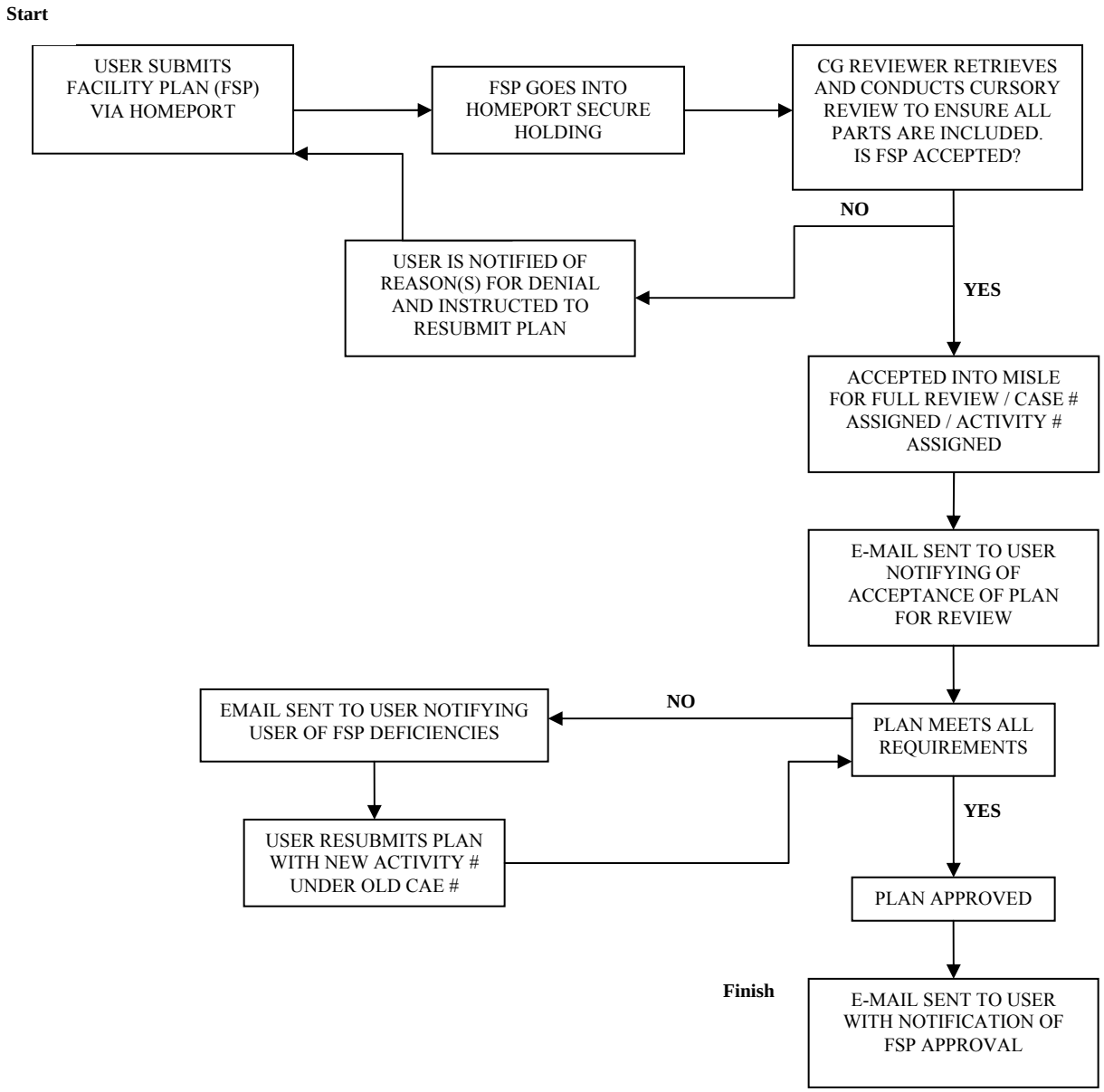


***NOTE 1: FSP SUBMITTER SHOULD BE ENCOURAGED TO EXPEDITE ALL NECESSARY REVISIONS AND TO RESUBMIT THE FSP IN A TIMELY MANNER. REGULATED OPERATIONS <u>CANNOT</u> COMMENCE WITHOUT AN APPROVED FSP.**

***NOTE 2: MAJOR AND MINOR REVISIONS ARE DEFINED IN ADDENDUM (3)**

Facility Security Plan (FSP)

HOMEPORT SUBMISSION, REVIEW, APPROVAL OR DENIAL



EXAMPLES OF MAJOR AND MINOR DEFICIENCIES

A. Major deficiencies noted during the review will require the plan to be return to the submitter for revision. Listed below are examples of major deficiencies:

1. An incomplete or missing facility vulnerability and security measures summary (form CG-6025)
2. An incomplete or missing FSA report,
3. Two or more incomplete FSP content requirements
4. Four or more FSP content items do not meet the intent of the regulations.

B. Minor deficiencies can occur more frequently than major deficiencies since they are on a smaller scale. Listed below are explains of minor deficiencies:

1. One required content section is missing or incomplete.
2. Facility contact information is not accurate/up-to-date.
3. There are no procedures for providing security training to personnel.
4. There are no procedures for changing MARSEC levels
5. Plan fails to provide an effective means to communicate on the facility.
6. There are no established security measures for restricted areas.

ENCLOSURE 2

GENERAL GUIDANCE FOR FSP PREPARERS AND REVIEWERS

GENERAL GUIDANCE FOR FACILITY SECURITY PLAN (FSP) PREPARERS AND REVIEWERS

2.1 Security Administration and Organization of the Facility

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

2.2 Personnel Training

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

2.3 Drills and Exercises

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

2.4 Records and Documentation

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

2.5 Response to Change in MARSEC Level

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

2.6 Communications

This section of the plan describes how the facility's communication systems are designed to accomplish security program requirements including notification, systems and procedures for effective and continuous communications. This section will include the processes/procedures used to accomplish individual requirements provided in **33 CFR Part 105.235.**

2.7 Procedures for Interfacing with Vessels

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

2.8 Declaration of Security (DoS)

This section of the plan will include a DoS as required in 33 CFR 101.505. It describes how the DoS is used during the vessel/facility interface as required by **33 CFR Part 105.245.**

2.9 Security Systems and Equipment Maintenance

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

2.10 Security Measures for Access Control, including designated public access areas
This section of the plan implements general security measures for access control at all MARSEC levels. This section describes in detail the security measures required by **33 CFR Part 105.255 and 257.** ***NOTE****: A MARSEC Directive could affect the performance standards contained this section.*

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

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

2.13 Security Measures for Delivery of Vessel Stores and Bunkers
This section of the plan must include general security measures for delivery of vessel stores and bunkers at all MARSEC levels. This section describes in detail the security measures as outlined in **33 CFR Part 105.270.** ***NOTE****: A MARSEC Directive could affect the performance standards contained this section.*

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

2.15 Security Incident Procedures
This section of the plan will include security incident procedures for each MARSEC level. This section describes in detail the security incident procedures required by **33 CFR Part 105.280.**

2.16 Audit and Security Plan Amendments
This section of the plan details how changes/amendments are made and audits are conducted at the facility. The plan will describe in detail the frequency and types, and how the amendments and audits are performed as required by **33 CFR Part 105.415.** Typically, any change requiring a new FSA will require an amendment to the FSP. Facility Security Officers are encouraged to electronically submit their FSP and FSP amendments directly to the local COTP on a password protected CD as Adobe or Word files. With COTP concurrence, FSPs or amendments may also be forwarded via Homeport. Administrative changes, such as phone numbers or a change in the name of the FSO or assistant FSO must be noted on the plan and forwarded to the COTP but do not require a new FSA or FSP amendments.

2.17 Facility Security Assessment (FSA) Report

This section of the plan contains written documentation of the FSA that is based on a collection of background information, the completion of an on-scene survey and an analysis of that information for the facility. An FSA report describes in detail the individual plan requirements in **33 CFR Part 105.300; 305 and 310.** *NOTE: in all cases, the FSA Report should be completed* ***prior to development of the FSP*** *as the FSP is the plan for mitigating all vulnerabilities first identified by the FSA.*

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

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

2.19 Additional Requirements for Passenger and Ferry Facilities

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

2.20 Additional Requirements for Cruise Ship Terminals

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

2.21 Additional Requirements for CDC Facilities

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

2.22 Additional Requirements for Barge Fleeting Facilities

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

ENCLOSURE 3

FACILITY SECURITY PLAN (FSP) REVIEW CHECKLIST FOR FSP PREPARERS AND REVIEWERS (GENERAL FACILITIES)

THIS PAGE WAS INTENTIONALLY LEFT BLANK

United States Coast Guard

FACILITY SECURITY PLAN (FSP) REVIEW CHECKLIST

Facility Name:	**Facility Type:**
Facility ID Number:	**MISLE Activity Number:**
Date(s) Conducted:	**CG Unit:**
1st Reviewer:	**2nd Reviewer:**

Guidance for completing the *Facility Security Plan (FSP) Review Checklist* –
Coast Guard facility inspectors shall complete the checklist by verifying the contents of the FSP submitted for review, are in line with the requirements as per 33 CFR 105.405. Each inspected item contained in the checklist must be notated as one of the following:

Satisfactory - Item meets requirements contained in the guide and referenced regulations.

Not Satisfactory - Item does not meet requirements in the guide and referenced regulations or is missing altogether.

Not Applicable - Item does not apply to this facility; the FSP should state why the regulatory provision is not applicable.

Sensitive Security Information (when filled out)

United States Coast Guard

FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

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

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

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

§105.405	***Yes***	***No***
(b) Was the FSP approved by the Coast Guard prior to March 26, 2007? **If yes; then it does not need to be amended to describe their TWIC procedures until the next regularly scheduled resubmission of the FSP.**	☐	☐
§105.405	***Complete***	***Incomplete***
(c) Review and evaluate the Facility Security Assessment (FSA) Report. **Ensure all identified vulnerabilities and information in the FSP concerning security measures in mitigation of these vulnerabilities have been identified and addressed in accordance with 33 CFR 105 Subpart C and 105.405(a)(18).**	☐	☐*

**Return FSP to submitter.*

Comments:

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(1) Security Administration and Organization of the Facility			
105.200 Owner or Operator (a) Each facility owner or operator must **ensure** that the facility operates in compliance with the requirements of this part.			
(b) For each facility, does the Facility Security Plan (FSP) **include** the following:			
(1) A defined security organization structure that identifies specific security duties and responsibilities;	☐	☐	☐
(2) FSO designation in writing with a 24-hour contact method;	☐	☐	☐
(3) Procedures to ensure that a Facility Security Assessment (FSA) is conducted;	☐	☐	☐
(4) Procedures to ensure the development and submission for approval of an FSP;	☐	☐	☐
(5) Procedures to ensure the facility operates in compliance with the approved FSP;	☐	☐	☐
(6) Procedures to ensure the TWIC program is properly implemented as set forth in this part, including:	☐	☐	☐
(i) Only authorized TWIC holders permitted to escort;	☐	☐	☐
(ii) Identifies actions an escort should take if escorted person engages in improper activities;	☐	☐	☐
(iii) Notifications of secure areas and public access areas of facility & the areas are clearly marked.	☐	☐	☐
(7) Procedures for ensuring restricted areas are controlled and TWIC provisions are coordinated, if applicable;	☐	☐	☐
(8) Procedures for coordinating security issues between the facility and vessels;	☐	☐	☐
(9) 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;	☐	☐	☐
(10) Procedures for implementing **MARSEC Level** security measures, within 12 hours of notification of an increase;	☐	☐	☐
(11) Procedures to ensure security for unattended vessels moored at the facility;	☐	☐	☐
(12) Procedures for reporting Breaches of Security and Transportation Security Incidents (TSI's) to the National Response Center in accordance with part 101 of this chapter;	☐	☐	☐
(13) Procedures to ensure consistency between security & safety requirements;	☐	☐	☐
(14) Procedures to ensure personnel are aware of the responsibilities of applying for and maintaining a TWIC per this part;	☐	☐	☐
(15) Procedures to ensure protocols with section 105.255(c) of this part, for dealing with individuals requiring access who report a lost, damaged, or stolen TWIC, or applied for but not yet received TWIC, are in place.	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
105.205 Facility Security Officer (FSO)			
(a) *General:*			
(1) Does the FSP **ensure** that the FSO is able to perform the duties and responsibilities required of the FSO?	☐	☐	☐
(2) If the same person serves as the FSO for more than one facility, does the FSP **identify** the facilities for which the FSO is designate, provided they are in the same COTP zone, not more than 50 miles apart, and the FSO is listed in each facility's FSP?	☐	☐	☐
(3) Does the FSP **ensure** that the FSO retains designated responsibilities although other individuals may perform specific tasks?	☐	☐	☐
(4) Does the FSP **identify** that the FSO must maintain a TWIC?	☐	☐	☐
(b) *Qualifications*:			
(1) Does the FSP **identify** the FSO as having knowledge/training in the following:			
(i) Security Organization of the facility;	☐	☐	☐
(ii) General vessel and facility operations and conditions;	☐	☐	☐
(iii) Vessel & facility security measures at all MARSEC levels;	☐	☐	☐
(iv) Emergency preparedness, response, and contingency planning;	☐	☐	☐
(v) Security equipment and systems, and their operational limits; and	☐	☐	☐
(vi) Methods of conducting audits, inspections, control, and monitoring techniques.	☐	☐	☐
(2) In addition to the above; the FSO must have knowledge/training in the following, *as appropriate*:			
(i) Relevant international laws and codes, and recommendations;	☐	☐	☐
(ii) Relevant government legislation and regulations;	☐	☐	☐
(iii) Responsibilities and functions of local, state, and federal law enforcement agencies;	☐	☐	☐
(iv) Security assessment methodology;	☐	☐	☐
(v) Methods of facility security surveys and inspections;	☐	☐	☐
(vi) Instruction techniques for security training and education, including security measures and procedures;	☐	☐	☐
(vii) Handling sensitive security information and security related communications;	☐	☐	☐
(viii) Current security threats and patterns;	☐	☐	☐
(ix) Recognizing and detecting dangerous substances and devices;	☐	☐	☐
(x) Recognizing characteristics and behavioral patterns of persons who are likely to threaten security;	☐	☐	☐
(xi) Techniques used to circumvent security measures;	☐	☐	☐
(xii) Conducting physical searches and non-intrusive inspections;	☐	☐	☐
(xiii) Conducting security drills and exercises, including exercises with vessels;	☐	☐	☐
(xiv) Assessing security drills and exercises; and	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(xv) Knowledge of TWIC requirements.	☐	☐	☐
(c) *Responsibilities:*			
(1) Does the FSP **identify** the following FSO responsibilities:	☐	☐	☐
(2) Ensuring the Facility Security Assessment (FSA) is conducted;	☐	☐	☐
(3) Ensuring development and implementation of a FSP;	☐	☐	☐
(4) Ensuring annual audit program is implemented and maintained at the facility;	☐	☐	☐
(5) Ensuring FSP is exercised per 105.220 of this part;	☐	☐	☐
(6) Ensuring regular security inspections of the facility are conducted;	☐	☐	☐
(7) Ensuring adequate security awareness and vigilance of the facility personnel;	☐	☐	☐
(8) Ensuring adequate training to personnel performing facility security duties;	☐	☐	☐
(9) Ensuring that occurrences that threaten the security of the facility are recorded and reported to the owner or operator;	☐	☐	☐
(10) Ensuring the maintenance of records required by this part;	☐	☐	☐
(11) Ensuring the preparation and submission of any reports as required by this part;	☐	☐	☐
(12) Ensuring the execution of any required Declarations of Security with Masters, Vessel Security Officers, or their designated representatives;	☐	☐	☐
(13) Ensuring the coordination of security services in accordance with the approved FSP;	☐	☐	☐
(14) Ensuring that security equipment is properly operated, tested, calibrated, and maintained;	☐	☐	☐
(15) Ensuring the recording and reporting of attainment changes in **MARSEC Levels** to the owner or operator and the cognizant COTP;	☐	☐	☐
(16) 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;	☐	☐	☐
(17) Ensuring notification to law enforcement and other emergency responders, as soon possible in order to permit a timely response to any transportation security incident;	☐	☐	☐
(18) 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;	☐	☐	☐
(19) Ensuring that all facility personnel are briefed of changes in security conditions at the facility; and	☐	☐	☐
(20) Ensure the TWIC program is being properly implemented.	☐	☐	☐
105.210 Facility Personnel With Security Duties Does the FSP **identify** a record keeping process to ensure that facility personnel responsible for security duties, maintain a TWIC, and have knowledge, through appropriate training or equivalent job experience in the following, *as appropriate:*			
(a) Knowledge of current security threats and patterns;	☐	☐	☐
(b) Recognition and detection of dangerous substances and devices;	☐	☐	☐
(c) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(d) Techniques used to circumvent security measures;	☐	☐	☐
(e) Crowd management and control techniques;	☐	☐	☐
(f) Security related communications;	☐	☐	☐
(g) Knowledge of emergency procedures and contingency plans;	☐	☐	☐
(h) Operation of security equipment and systems;	☐	☐	☐
(i) Testing, calibration, and maintenance of security equipment and systems;	☐	☐	☐
(j) Inspection, control, and monitoring techniques;	☐	☐	☐
(k) Relevant provisions of the Facility Security Plan (FSP);	☐	☐	☐
(l) Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores;	☐	☐	☐
(m) The meaning and the consequential requirements of the different **MARSEC Levels;** and	☐	☐	☐
(n) Familiarity with all relevant aspects of the TWIC program and how to carry them out.	☐	☐	☐
(2) Personnel Training			
105.215 Security Training for all Other Facility Personnel			
Does the FSP **identify** procedures or policies to ensure personnel, including contractors, whether part-time, full-time, temporary, or permanent, have knowledge of, through training or equivalent job experience, in the following, *as appropriate*:			
(a) Relevant provisions of the Facility Security Plan (FSP);	☐	☐	☐
(b) The meaning and the consequential requirements of the different MARSEC Levels as they apply to them, including emergency procedures and contingency plans;	☐	☐	☐
(c) Recognition and detection of dangerous substances and devices;	☐	☐	☐
(d) Recognition of characteristics and behavioral patterns of persons who are likely to threaten security;	☐	☐	☐
(e) Techniques used to circumvent security measures; and	☐	☐	☐
(f) Familiarity with all relevant aspects of the TWIC program and how to carry them out.	☐	☐	☐
(3) Drills and Exercises			
105.220 Drill and Exercise Requirements (a) *General*:			
(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?	☐	☐	☐
(2) Does the FSP **direct** the Facility Security Officer (FSO) to identify related security deficiencies identified during drills and exercise?	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(b) *Drills:*			
(1) 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) 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?	☐	☐	☐
(c) *Exercises:*			
(1) Does the FSP **require** that exercises must be conducted at least once each calendar year, with no more than 18 months between exercises?	☐	☐	☐
(2) Does the FSP explain that exercises may consist of:			
(i) Full scale or live;	☐	☐	☐
(ii) Tabletop simulation or seminar;	☐	☐	☐
(iii) Combined with other appropriate exercises; or	☐	☐	☐
(iv) A combination of the elements in paragraphs (c)(2)(i) through (iii) of this section.	☐	☐	☐
(3) Does the FSP identify that exercises can be either facility-specific or part of a cooperative exercise program with applicable facility and vessel security plans or comprehensive port exercises?	☐	☐	☐
(4) Does the FSP identify exercises that test communication and notification procedures, and elements of coordination, resource availability, and response?	☐	☐	☐
(5) Does the FSP identify exercises that test the entire security program and include substantial and active participation of FSOs and others, as appropriate?	☐	☐	☐
(4) Records and Documentation			
105.225 Facility Recordkeeping Requirements (a) Does the FSP direct the FSO to keep records of the activities as set out in paragraph (b) of this section for at least 2 years and make them available to the Coast Guard upon request?	☐	☐	☐
(b) If the records are kept in an electronic format, does the FSP detail how they are protected against unauthorized deletion, destruction, or amendment?	☐	☐	☐
* *Have procedures been identified to maintain the following records:*			
(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) 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 that may improve the FSP	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(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 breach, to whom it was reported, and description of the response.	☐	☐	☐
(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	☐	☐	☐
(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	☐	☐	☐
(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	☐	☐	☐
(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	☐	☐	☐
(8) Annual audit of the FSP. For each annual audit, a letter certified by the FSO stating the date the audit was completed	☐	☐	☐
(c) Does the FSP include procedures to protect records from unauthorized access or disclosure?	☐	☐	☐
(5) Response to Change in MARSEC Level			
105.230 Maritime Security (MARSEC) Level Coordination and Implementation (a) Does the FSP identify procedures to ensure that the facility operates in compliance with the security requirements for the **MARSEC Level** in effect for the port?	☐	☐	☐
(b) When notified of an increase in the **MARSEC Level,** does the FSP direct the facility owner and operator to ensure that:			
(1) Vessels moored to the facility and vessels scheduled to arrive at the facility within 96 hours of the **MARSEC Level** change are notified of the new **MARSEC Level** and the Declaration of Security is revised as necessary	☐	☐	☐
(2) The facility complies with the required additional security measures within 12 hours	☐	☐	☐
(3) The facility reports compliance or noncompliance to the COTP	☐	☐	☐
(c) 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?	☐	☐	☐
(d) 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 increased MARSEC level?	☐	☐	☐
(e) 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:			

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(1) Use of waterborne security patrol;	☐	☐	☐
(2) Use of armed security personnel to control access to the facility and to deter, to the maximum extent practical, a transportation security incident; and	☐	☐	☐
(3) Examination of piers, wharves, and similar structures at the facility for the presence of dangerous substances or devices underwater or other threats.	☐	☐	☐
(6) Procedures for Interfacing with Vessels			
105.240 Procedures for interfacing with vessels Does the FSP ensure that there are measures for interfacing with vessels at all **MARSEC Levels?**	☐	☐	☐
(7) Declaration of Security (DoS)			
105.245 Declaration of Security (DoS) (a) Does the FSP ensure procedures are established for requesting a DoS and for handling DoS requests from a vessel?	☐	☐	☐
(b) Does the FSP, at **MARSEC Level 1,** ensure a facility receiving a cruise ship or a manned vessel carrying Certain Dangerous Cargo (CDC), in bulk, comply with the following:			
(1) The FSO, prior to the arrival of a vessel to the facility, ensures 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; and	☐	☐	☐
(2) Upon the arrival of the vessel at the facility, the FSO and Master, VSO, or their designated representative, must sign the written DoS.	☐	☐	☐
(c) 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?	☐	☐	☐
(d) Does the FSP at **MARSEC Levels 2 and 3** require the FSOs, or their designated representatives, of facilities interfacing with manned vessels subject to part 104, of this subchapter to sign and implement DoS documents as required in (b)(1) and (2) of this section?	☐	☐	☐
(e) Does the FSP at **MARSEC Levels 1 and 2** indicate that the FSOs of facilities interfacing with the same vessels may implement a continuing DoS for multiple visits, providing that:			
(1) The DoS is valid for a specific **MARSEC Level**	☐	☐	☐
(2) The effective period at **MARSEC Level 1** does not exceed 90 days	☐	☐	☐
(3) The effective period at **MARSEC Level 2** does not exceed 30 days	☐	☐	☐
(f) Does the FSP identify that when the **MARSEC Level** increases beyond that contained in the DoS or the continuing DoS, that it is void and new DoS must be executed?	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard

FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(g) Does the FSP ensure a copy of all currently valid continuing DoS documents be kept with the Facility Security Plan?	☐	☐	☐
(h) Does the FSP state that the COTP may require a DoS at any time, at any MARSEC level?	☐	☐	☐
(8) Communications			
105.235 Communications (a) Does the FSP provide a means to effectively notify facility personnel of changes in security conditions at the facility?	☐	☐	☐
(b) 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?	☐	☐	☐
(c) Does the FSP identify at each active facility access point, a means of contacting police, security control, or an emergency operations center, by telephones, cellular phones, portable radios, or other equivalent means?	☐	☐	☐
(d) Does the FSP ensure facility communications systems have a backup means for both internal and external communications?	☐	☐	☐
(9) Security Systems and Equipment Maintenance			
105.250 Security Systems and Equipment Maintenance (a) Does the FSP include procedures to ensure Security systems and equipment are in good working order and are inspected, tested, calibrated, and maintained according to manufacturers' recommendations?	☐	☐	☐
(b) 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 in part 105.225 of this subpart?	☐	☐	☐
(c) Does the FSP include procedures for identifying and responding to security system and equipment failures or malfunctions?	☐	☐	☐
(10) Security Measures for Access Control			
105.255 Security Measures for Access Control (a) Does the FSP have procedures to ensure the implementation of security measures to:			
(1) Deter the unauthorized introduction of dangerous substances and devices, including any device intended to damage or destroy persons, vessels, facilities, or ports;	☐	☐	☐
(2) Secure dangerous substances and devices that are authorized by the owner or operator to be on the facility;	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(3) Control access to the facility; and	☐	☐	☐
(4) Prevent an unescorted individual from entering an area of the facility that is designated as a secure area unless the individual holds a duly issued TWIC and is authorized to be in the area.	☐	☐	☐
(b) Does the FSP ensure that:			
(1) The locations where there are restrictions or prohibitions that prevent unauthorized access are applied for each MARSEC level, including those points where TWIC access control provisions will be applied. Each location allowing means of gaining access to the facility must be addressed;	☐	☐	☐
(2) The types of restriction or prohibitions to be applied and the means of enforcing them are identified;	☐	☐	☐
(3) The means used to establish the identity of individuals not in possession of a TWIC, in accordance with 101.515 of this subchapter, and procedures for escorting them;	☐	☐	☐
(4) Procedures for identifying authorized and unauthorized persons at any MARSEC level;	☐	☐	☐
(5) 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;	☐	☐	☐
(c) Does the Facility owner or operator ensure that a TWIC program is implemented as follows:	☐	☐	☐
(1) All persons seeking unescorted access to secure areas must present their TWIC for inspection before being allowed unescorted access, in accordance with section 101.514 of this subchapter. Inspection must include:			
(i) A match of the photo on the TWIC to the individual presenting the TWIC;	☐	☐	☐
(ii) Verification that the TWIC has not expired; and	☐	☐	☐
(iii) A visual check of the various security features present on the card to ensure that the TWIC has not been forged or tampered.	☐	☐	☐
(2) If an individual cannot present a TWIC because it has been lost or stolen, and he or she has previously been granted unescorted access to the facility and is known to have had a valid TWIC, the individual may be given unescorted access to secure areas for a period of no longer than 7 consecutive calendar days if:			
(i) The individual has reported the TWIC as lost or stolen to TSA as required by 49 CFR 1572.21;	☐	☐	☐
(ii) The individual can present another identification credential that meets the requirements of section 101.515 of this subchapter; and	☐	☐	☐
(iii) There are no suspicious circumstances associated with the individual's claim of loss or theft.	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(3) If the individual cannot present his or her TWIC for any other reason than outlined in paragraph (c)(2) of this section, he or she may not be granted unescorted access to the secure area. The individual must be under escort, as that term is defined in part 101 of this subchapter, at all times when inside of a secure area.	☐	☐	☐
(4) With the exception of persons granted access according to paragraph (c)(2) of this section, all persons granted unescorted access to secure areas of the facility must be able to produce his or her TWIC upon request.	☐	☐	☐
(5) Uses disciplinary measures to discourage fraud and abuse.	☐	☐	☐
(6) The facility's TWIC program should be coordinated, when practicable, with identification and TWIC access control measures of vessels or other transportation conveyances that use the facility.	☐	☐	☐
(d) If the Facility owner or operator uses a separate identification system, does the FSP ensure that it complies and is coordinated with TWIC provisions in this part?	☐	☐	☐
(e) Does the FSP establish the frequency of application of any access controls, particularly if they are to be applied on a random or occasional basis?	☐	☐	☐
(f) *MARSEC Level 1:* Does the FSP at **MARSEC Level 1** ensure the following security measures are implemented at the facility:			
(1) Implemented TWIC as set out in paragraph (c) of this section.	☐	☐	☐
(2) Screen persons, baggage (including carry-on items), personal effects, and 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;	☐	☐	☐
(3) Have signs been conspicuously posted describing the security measures in effect and state:			
(i) Entering the facility is deemed valid consent to screening or inspection; and	☐	☐	☐
(ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter.	☐	☐	☐
(4) Check the identification of any person not holding a TWIC and seeking entry to the facility, including vessel passengers, vendors, personnel duly authorized by the cognizant government authorities, and visitors. This check shall include confirming the reason for entering by examining at least one of the following:			
(i) Joining instructions	☐	☐	☐
(ii) Passenger tickets	☐	☐	☐
(iii) Boarding passes	☐	☐	☐
(iv) Work orders, pilot orders, or surveyor orders	☐	☐	☐
(v) Government identification	☐	☐	☐
(vi) Visitor badges issued in accordance with an identification system implemented in accordance with the rules of this section	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard

FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(5) 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 or a law enforcement officer, to establish his or her identity in accordance with this part or to account for his or her presence. Any such incident must be reported in compliance with this part;	☐	☐	☐
(6) Designate restricted areas and provide appropriate access controls for these areas;	☐	☐	☐
(7) Identify access points that must be secured or attended to deter unauthorized access;	☐	☐	☐
(8) Deter unauthorized access to the facility and to designated restricted areas within the facility;	☐	☐	☐
(9) Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel; and	☐	☐	☐
(10) Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between the facility and a vessel.	☐	☐	☐
(g) *MARSEC Level 2:* In addition to the security measures required for **MARSEC Level 1**, does the FSP ensure the implementation of additional security measures, as specified for **MARSEC Level 2**, that may include:			
(1) Increasing the frequency and detail of the screening of persons, baggage, and personal effects for dangerous substances and devices entering the facility	☐	☐	☐
(2) X-ray screening of all unaccompanied baggage	☐	☐	☐
(3) Assigning additional personnel to guard access points and patrol the perimeter of the facility to deter unauthorized access	☐	☐	☐
(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	☐	☐	☐
(5) Denying access to visitors who do not have a verified destination	☐	☐	☐
(6) Deterring waterside access to the facility, which may include using waterborne patrols to enhance security around the facility	☐	☐	☐
(7) Except for government-owned vehicles on official business when government personnel present identification credentials for entry, screening vehicles and their contents for dangerous substances and devices at the rate specified for **MARSEC Level 2** in the approved FSP	☐	☐	☐
(h) *MARSEC Level 3:* In addition to the security measures required for **MARSEC Levels 1 and 2,** in this section**,** at **MARSEC Level 3** does the FSP ensure the implementation of additional security measures that may include:			
(1) Screening all persons, baggage, and personal effects for dangerous substances and devices;	☐	☐	☐
(2) Performing one or more of the following on unaccompanied baggage:			
(i) Screen unaccompanied baggage more extensively; for example, x-raying from two or more angles	☐	☐	☐
(ii) Prepare to restrict or suspend handling unaccompanied baggage	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(iii) Refuse to accept unaccompanied baggage	☐	☐	☐
(3) Being prepared to cooperate with responders and other facilities	☐	☐	☐
(4) Granting access to only those responding to a security incident or threat	☐	☐	☐
(5) Suspending access to the facility	☐	☐	☐
(6) Suspending cargo operations	☐	☐	☐
(7) Evacuating the facility	☐	☐	☐
(8) Restricting pedestrian or vehicular movement on the grounds of the facility	☐	☐	☐
(9) Increasing security patrols within the facility	☐	☐	☐
105.257 Security Measures for Newly-Hired Employees Does the FSP address the following TWIC rules in accordance with regulations?	☐	☐	☐
(a) Newly-hired facility employees may be granted entry to secure areas of the facility for up to 30 consecutive calendar days prior to receiving their TWIC provided all of the requirements in this section are met, and provided that the new hire is accompanied by an individual with a TWIC while within the secure areas of the facility.	☐	☐	☐
(b) Newly-hired facility employees and FSO have completed the following prior to access being granted:			
(1) The new hire has applied for a TWIC in accordance with 49 CFR Part 1572 by completing the full enrollment process, paying the user fee, and not be currently engaged in a waiver or appeal process. The facility owner or operator or the Facility Security Officer (FSO) must have the new hire sign a statement affirming this, and must retain the signed statement until the new hire receives a TWIC; and	☐	☐	☐
(2) The facility owner or operator or the FSO enters the following information on the new hire into the Coast Guard's Homeport website (http://homeport.uscg.mil):			
(i) Full legal name, including middle name if one exists;	☐	☐	☐
(ii) Date of birth;	☐	☐	☐
(iii) Social security number (optional);	☐	☐	☐
(iv) Employer name and 24 hour contact information; and	☐	☐	☐
(v) Date of TWIC enrollment.	☐	☐	☐
(3) The new hire presents an identification credential that meets the requirements of 101.515 of this subchapter.	☐	☐	☐
(4) There are no other circumstances that would cause reasonable suspicion regarding the new hire's ability to obtain a TWIC, and the facility owner or operator or FSO have not been informed by the cognizant COTP that the new hire poses a security threat.	☐	☐	☐
(5) There would be an adverse impact to facility operations if the new hire is not allowed access.	☐	☐	☐
(c) This section does not apply to any individual being hired as a FSO, or any individual being hired to perform facility security duties.	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard

FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(d) The new hire may not begin working at the facility under the provisions of this section until the owner, operator, or FSO receives notification, via Homeport or some other means, the new hire has passed an initial name check.	☐	☐	☐
(11) Security Measures for Restricted Areas			
105.260 Security Measures for Restricted Areas (a) *General:* Does the FSP ensure the designation of restricted areas in order to:			
(1) Prevent or deter unauthorized access	☐	☐	☐
(2) Protect persons authorized to be in the facility	☐	☐	☐
(3) Protect the facility	☐	☐	☐
(4) Protect vessels using and serving the facility	☐	☐	☐
(5) Protect sensitive security areas within the facility	☐	☐	☐
(6) Protect security and surveillance equipment and systems	☐	☐	☐
(7) Protect cargo and vessel stores from tampering	☐	☐	☐
(b) *Designation of Restricted Areas:* 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:	☐	☐	☐
(1) Shore areas immediately adjacent to each vessel moored at the facility	☐	☐	☐
(2) Areas containing sensitive security information, including cargo documentation	☐	☐	☐
(3) Areas containing security and surveillance equipment and systems and their controls, and lighting system controls	☐	☐	☐
(4) Areas containing critical facility infrastructure, including:			
(i) Water supplies	☐	☐	☐
(ii) Telecommunications	☐	☐	☐
(iii) Electrical system	☐	☐	☐
(iv) Access points for ventilation and air-conditioning systems	☐	☐	☐
(5) Manufacturing or processing areas and control rooms	☐	☐	☐
(6) Locations in the facility where access by vehicles and personnel should be restricted	☐	☐	☐
(7) Areas designated for loading, unloading or storage of cargo and stores	☐	☐	☐
(8) Areas containing cargo consisting of dangerous goods or hazardous substances, including certain dangerous cargoes	☐	☐	☐
(c) Does the FSP have processes that ensure that all restricted areas have clearly established security measures to:			
(1) Identify which facility personnel are authorized to have access	☐	☐	☐
(2) Determine which persons other than facility personnel are authorized to have access	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(3) Determine the conditions under which that access may take place	☐	☐	☐
(4) Define the extent of any restricted area	☐	☐	☐
(5) Define the times when access restrictions apply	☐	☐	☐
(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	☐	☐	☐
(7) Control the entry, parking, loading and unloading of vehicles	☐	☐	☐
(8) Control the movement and storage of cargo and vessel stores	☐	☐	☐
(9) Control unaccompanied baggage or personal effects	☐	☐	☐
(d) *MARSEC Level 1:* Does the FSP, at **MARSEC Level 1,** ensure the implementation of security measures to prevent unauthorized access or activities within the area that may include:			
(1) Restricting access to only authorized personnel	☐	☐	☐
(2) Securing all access points not actively used and providing physical barriers to impede movement through the remaining access points	☐	☐	☐
(3) Assigning personnel to control access to restricted areas	☐	☐	☐
(4) Verifying the identification and authorization of all persons and all vehicles seeking entry	☐	☐	☐
(5) Patrolling or monitoring the perimeter of restricted areas	☐	☐	☐
(6) Using security personnel, automatic intrusion detection devices, surveillance equipment or systems to detect unauthorized entry or movement within restricted areas	☐	☐	☐
(7) Directing the parking, loading, and unloading of vehicles within a restricted area	☐	☐	☐
(8) Controlling unaccompanied baggage and/or personal effects after screening	☐	☐	☐
(9) Designating restricted areas for performing inspections of cargo and vessel stores while awaiting loading	☐	☐	☐
(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	☐	☐	☐
(e) *MARSEC Level 2:* 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 that may include:			
(1) Increasing the intensity and frequency of monitoring and access controls on existing restricted access areas	☐	☐	☐
(2) Enhancing the effectiveness of the barriers or fencing surrounding restricted areas, by the use of patrols or automatic intrusion detection devices	☐	☐	☐
(3) Reducing the number of access points to restricted areas, and enhancing the controls applied at the remaining accesses	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard

FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(4) Restricting parking adjacent to vessels	☐	☐	☐
(5) Further restricting access to the restricted areas and movements and storage within them	☐	☐	☐
(6) Using continuously monitored and recorded surveillance equipment	☐	☐	☐
(7) Enhancing the number and frequency of patrols, including waterborne patrols undertaken on the boundaries of the restricted areas and within the areas	☐	☐	☐
(8) Establishing and restricting access to areas adjacent to the restricted areas	☐	☐	☐
(f) *MARSEC Level 3:* Does the FSP at **MARSEC Level 3,** in addition to the security measures required for **MARSEC Levels 1 and 2,** ensure the implementation of additional security measures that may include:			
(1) Restricting access to additional areas;	☐	☐	☐
(2) Prohibiting access to restricted areas; and	☐	☐	☐
(3) Searching restricted areas as part of a security sweep of all or part of the facility.	☐	☐	☐
(12) Security Measures for Handling Cargo			
105.265 Security Measures for Handling Cargo (a) *General:* 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) Deter tampering	☐	☐	☐
(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	☐	☐	☐
(3) Identify cargo that is approved for loading onto vessels interfacing with the facility	☐	☐	☐
(4) Include cargo control procedures at access points to the facility	☐	☐	☐
(5) Identify cargo that is accepted for temporary storage in a restricted area while awaiting loading or pick up	☐	☐	☐
(6) Restrict the entry of cargo to the facility that does not have a confirmed date for loading, as appropriate.	☐	☐	☐
(7) Ensure the release of cargo only to the carrier specified in the cargo documentation.	☐	☐	☐
(8) Coordinate security measures with the shipper or other responsible party in accordance with an established agreement and procedures.	☐	☐	☐
(9) Create, update, and maintain a continuous inventory, including location, of all dangerous goods or hazardous substances from receipt to delivery within the facility, giving the location of those dangerous goods or hazardous substances.	☐	☐	☐
(b) *MARSEC Level 1:* Does the FSP at **MARSEC Level 1** ensure the implementation of measures to:			
(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) Check that cargo, containers, or other cargo transport units entering the facility match the delivery note or equivalent cargo documentation.	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard

FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(3) Screen vehicles	☐	☐	☐
(4) Check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility.	☐	☐	☐
(c) *MARSEC Level 2:* 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 that may include:			
(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) Intensifying the screening of vehicles.	☐	☐	☐
(4) Increasing frequency and detail in checking of seals and other methods used to prevent tampering.	☐	☐	☐
(5) Segregating inbound cargo, outbound cargo, and vessel stores.	☐	☐	☐
(6) Increasing the frequency and intensity of visual and physical inspections.	☐	☐	☐
(7) Limiting the number of locations where dangerous goods and hazardous substances, including certain dangerous cargoes, can be stored.	☐	☐	☐
(d) *MARSEC Level 3:* Does the FSP at **MARSEC Level 3,** in addition to the security measures required for **MARSEC Levels 1 and 2,** ensure the implementation of additional security measures that may include:			
(1) Restricting or suspending cargo movements or operations within all or part of the facility or specific vessels	☐	☐	☐
(2) Being prepared to cooperate with responders and vessels	☐	☐	☐
(3) Verifying the inventory and location of any dangerous goods and hazardous substances, including certain dangerous cargoes, held within the facility and their location	☐	☐	☐
(13) Security Measures for Delivery of Vessel Stores and Bunkers			
105.270 Security Measures for Delivery of Vessel Stores and Bunkers (a) *General:* Does the FSP ensure that security measures relating to the delivery of vessel stores and bunkers are implemented to:			
(1) Check vessel stores for package integrity;	☐	☐	☐
(2) Prevent vessel stores from being accepted without inspection;	☐	☐	☐
(3) Deter tampering;	☐	☐	☐
(4) 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; and	☐	☐	☐
(5) Check vessel stores by one of the following means:			
(i) Visual examination;	☐	☐	☐
(ii) Physical examination;	☐	☐	☐
(iii) Detection devices, such as scanners; or	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard

FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(iv) Canines	☐	☐	☐
(b) *MARSEC Level 1:* Does the approved FSP at **MARSEC Level 1** ensure the implementation of measures to:			
(1) Screen vessel stores at the rate specified;	☐	☐	☐
(2) Require advance notification of vessel stores or bunkers delivery, including a list of stores, delivery vehicle driver information, and vehicle registration information;	☐	☐	☐
(3) Screen delivery vehicles at the frequencies specified; or	☐	☐	☐
(4) Escort delivery vehicles within the facility at the rate specified.	☐	☐	☐
(c) *MARSEC Level 2:* 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 that may include:			
(1) Detailed screening of vessel stores;	☐	☐	☐
(2) Detailed screening of all delivery vehicles;	☐	☐	☐
(3) Coordinating with vessel personnel to check the order against the delivery note prior to entry to the facility;	☐	☐	☐
(4) Ensuring delivery vehicles are escorted within the facility; or	☐	☐	☐
(5) Restricting or prohibiting the entry of vessel stores that will not leave the facility within a specified period.	☐	☐	☐
(d) *MARSEC Level 3:* Does the FSP at **MARSEC Level 3,** in addition to the security measures required for **MARSEC Levels 1 and 2,** ensure the implementation of additional security measures that may include:			
(1) Checking all vessel stores more extensively;	☐	☐	☐
(2) Restricting or suspending delivery of vessel stores; or	☐	☐	☐
(3) Refusing to accept vessel stores on the facility.	☐	☐	☐
(14) Security Measures for Monitoring			
105.275 Security Measures for Monitoring (a) *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) Facility and its nearby approaches, on land and water;	☐	☐	☐
(2) Restricted areas within the facility; and	☐	☐	☐
(3) Vessels at the facility and/or areas surrounding the vessels.	☐	☐	☐
(b) *MARSEC Level 1:* Does the approved FSP at **MARSEC Level 1** ensure the security measures in this section are implemented at all times, including the period from sunset to sunrise and periods of limited visibility. For each facility, ensure monitoring capability that:			

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(1) When automatic intrusion-detection devices are used, an audible or visual alarm is activated that is either continuously attended or monitored;	☐	☐	☐
(2) Provisions for monitoring equipment to function continually, including consideration of the possible effects of weather or of a power disruption;	☐	☐	☐
(3) Monitors the facility area, including shore and waterside access to it;	☐	☐	☐
(4) The capability of monitors access points, barriers and restricted areas;	☐	☐	☐
(5) The capability of monitors access and movements adjacent to vessels using the facility, including augmentation of lighting provided by the vessel itself; and	☐	☐	☐
(6) Provisions to limit lighting effects, such as glare, and their impact on safety, navigation, and other security activities.	☐	☐	☐
(c) *MARSEC Level 2:* 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 that may include:			
(1) Increasing the coverage and intensity of surveillance equipment, including the provision of additional surveillance coverage;	☐	☐	☐
(2) Increasing the frequency of foot, vehicle or waterborne patrols;	☐	☐	☐
(3) Assigning additional security personnel to monitor and patrol; or	☐	☐	☐
(4) Increasing the coverage and intensity of lighting, including the provision of additional lighting and coverage.	☐	☐	☐
(d) *MARSEC Level 3:* Does the FSP at **MARSEC Level 3,** in addition to the security measures required for **MARSEC Levels 1 and 2,** ensure the implementation of additional security measures that may include:			
(1) Switching on all lighting within, or illuminating the vicinity of, the facility?	☐	☐	☐
(2) Switching on all surveillance equipment capable of recording activities within or adjacent to the facility?	☐	☐	☐
(3) Maximizing the length of time such surveillance equipment can continue to record?	☐	☐	☐
(4) A description of procedures to comply with the instructions issued by those responding to the security incident?	☐	☐	☐
(15) Security Incident Procedures			
105.280 Security Incident Procedures			
For each **MARSEC Level**, Does the Facility Security Plan (FSP) ensure that the Facility Security Officer (FSO) and facility security personnel are able to:			
(a) Respond to security threats or breaches of security and maintain critical facility and vessel-to-facility interface operations;	☐	☐	☐
(b) Evacuate the facility in case of security threats or breaches of security;	☐	☐	☐
(c) Report security incidents as required in 101.305 of this subchapter;	☐	☐	☐
(d) Brief all facility personnel on possible threats and the need for vigilance, soliciting their assistance in reporting suspicious persons, objects, or activities; and	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard

FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(e) Secure non-critical operations in order to focus response on critical operations.	☐	☐	☐
(16) Audits and Security Plan Amendments			
105.415 Amendment and Audit			
(a) *Amendments:* Does the FSP identify the amendment procedures to a Facility Security Plan (FSP) that is approved by the cognizant COTP or proposed amendments submitted to the cognizant COTP by the Facility owner or operator per 105.415(a)(1) through (4) of this subpart?	☐	☐	☐
(b) *Audits:* Does the FSP define the audit process, describe who will conduct the audit, their experience/knowledge level, and procedures to perform audits when amendments have been made to the FSP per 105.415(b)(1) through (5) of this subpart?	☐	☐	☐
(17) Facility Security Assessment (FSA) Report			
105.305 Facility Security Assessment (FSA) Requirements (Subpart C)			
(c) *FSA Report:*			
(1) Verify the written FSA report is prepared and included as part of the FSP, and must contain the following:			
(i) A summary of how the on-scene survey was conducted;	☐	☐	☐
(ii) A description of existing security measures, including inspection, control and monitoring equipment, personnel identification documents and communication, alarm, lighting, access control, and similar systems;	☐	☐	☐
(iii) A description of each vulnerability found during the on-scene survey;	☐	☐	☐
(iv) A description of security measures that could be used to address each vulnerability;	☐	☐	☐
(v) A list of the key facility operations that are important to protect; and	☐	☐	☐
(vi) 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:			
(i) Physical security;	☐	☐	☐
(ii) Structural integrity;	☐	☐	☐
(iii) Personnel protection systems;	☐	☐	☐
(iv) Procedural policies;	☐	☐	☐
(v) Radio and telecommunication systems, including computer systems and networks;	☐	☐	☐
(vi) Relevant transportation infrastructure; and	☐	☐	☐
(vii) 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:			
(i) Facility personnel;	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(ii) Passengers, visitors, vendors, repair technicians, vessel personnel, etc;	☐	☐	☐
(iii) Capacity to maintain emergency response;	☐	☐	☐
(iv) Cargo, particularly dangerous goods and hazardous substances;	☐	☐	☐
(v) Delivery of vessel stores;	☐	☐	☐
(vi) Any facility security communication and surveillance systems; and	☐	☐	☐
(vii) Any other facility security systems, if any.	☐	☐	☐
(4) Does the FSA report account for the vulnerabilities in the following areas:			
(i) Conflicts between safety and security measures?	☐	☐	☐
(ii) Conflicts between duties and security assignments?	☐	☐	☐
(iii) The impact of watch-keeping duties and risk of fatigue on facility personnel alertness and performance?	☐	☐	☐
(iv) Security training deficiencies?	☐	☐	☐
(v) Security equipment and systems, including communication systems?	☐	☐	☐
(5) Does the FSA report discuss and evaluate key facility measures and operations, including:			
(i) Ensuring performance of all security duties	☐	☐	☐
(ii) Controlling access to the facility, through the use of identification systems or otherwise;	☐	☐	☐
(iii) Controlling the embarkation of vessel personnel and other persons and their effects (including personal effects and baggage whether accompanied or unaccompanied);	☐	☐	☐
(iv) Procedures for the handling of cargo and the delivery of vessel stores;	☐	☐	☐
(v) Monitoring restricted areas to ensure that only authorized persons have access;	☐	☐	☐
(vi) Monitoring the facility and areas adjacent to the pier.	☐	☐	☐
(18) Facility Vulnerability and Security Measures Summary - Example of Form CG-6025 is in Appendix A to Part 105 -			
105.405 Facility Vulnerability and Security Measures Summary (Form CG-6025)			
Has the Facility Vulnerability and Security Measures Summary (Form CG-6025) been completed using the following?			
● Information found in the FSA concerning identified vulnerabilities; and	☐	☐	☐
● Information found in the FSP concerning security measures in mitigation of these vulnerabilities.	☐	☐	☐
● Does the CG-6025 list the vulnerabilities identified from the above?	☐	☐	☐
§105.285 – 296 Additional Requirements Sections			
105.285 Additional Requirements – Passenger and Ferry Facilities			
(a) Does the FSP identify, at all **MARSEC Levels**, the security measures that have been established in coordination with a vessel moored at the facility by:			

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(1) Establishing separate areas for segregation of checked from unchecked persons and personal effects	☐	☐	☐
(2) Assuring a defined percentage of vehicles to be loaded are screened prior to loading in accordance with current MARSEC Directive or orders issued by the Coast Guard	☐	☐	☐
(3) Assuring that all unaccompanied vehicles are screened prior to loading	☐	☐	☐
(4) Denying passengers access to security and restricted areas unless supervised by facility personnel	☐	☐	☐
(5) Providing sufficient security personnel to monitor all persons in a facility with a public access area designated under 105.106	☐	☐	☐
(b) At **MARSEC Level 2**, in addition to the requirements stated paragraph (a) of this section, the owner or operator of a passenger or ferry facility with a public access area designated under 105.106 must increase the intensity of monitoring of the public access area	☐	☐	☐
(c) At **MARSEC Level 3**, in addition to the requirements stated paragraphs (a) and (b) of this section, the owner or operator of a passenger or ferry facility with a public access area designated under 105.106 must increase the intensity of monitoring and assign additional security personnel to monitor the public access area	☐	☐	☐
105.290 Additional Requirements – Cruise Ship Terminals			
At all **MARSEC Levels,** the facility owner or operator, in coordination with a vessel moored at the facility, must ensure the following security measures by:			
(a) Screening all persons, baggage, and personal effects for dangerous substances and devices;	☐	☐	☐
(b) Checking the identification of all persons seeking to board the vessel. Persons holding a TWIC shall be checked as set forth in this part. For those not holding a TWIC this check includes confirming the reason for boarding by examining joining instructions, passenger tickets, boarding passes, government identification or visitor badges, or work orders;	☐	☐	☐
(c) Designate holding, waiting, or embarkation areas within the facility's secure area to segregate screened persons and their personal effects from unscreened persons and their personal effects;	☐	☐	☐
(d) Providing additional security personnel to designated holding, waiting, or embarkation areas within the facility's secure area; and	☐	☐	☐
(e) Denying individuals not holding a TWIC access to secure and restricted areas unless escorted.	☐	☐	☐
105.295 Additional Requirements – Certain Dangerous Cargo (CDC) Facilities			
(a) At all **MARSEC Levels**, in addition to requirements of this part, owners or operators of CDC facilities must ensure the implementation of the following security measures by :			

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

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

FSP Content Requirements per 33 CFR 105.405(a): ** Note: Does the FSP briefly state why the regulatory provision is not applicable?*	***Satisfactory***	***Not Satisfactory***	****Not Applicable***
(2) Controlling the parking, loading, and unloading of vehicles within a facility;	☐	☐	☐
(3) Requiring security personnel to record or report their presence at key points during their patrols;	☐	☐	☐
(4) Searching unmanned or unmonitored waterfront areas for dangerous substances and devices prior to a vessel's arrival at the facility; and	☐	☐	☐
(5) Providing an alternate or independent power source for security and communications systems.	☐	☐	☐
(b) At **MARSEC Level 2**, in addition to requirements of **MARSEC Level 1,** owners or operators of CDC facilities must ensure the implementation of the following security measures by:			
(1) Releasing of cargo only in the presence of the Facility Security Officer (FSO) or a designated representative of the FSO;	☐	☐	☐
(2) Continuously patrolling of restricted areas:	☐	☐	☐
(c) At **MARSEC Level 3**, in addition to requirements of **MARSEC Level 1 and 2**, owners or operators of CDC facilities must ensure the facilities are continuously guarded and restricted areas are patrolled.	☐	☐	☐
105.296 Additional Requirements – Barge Fleeting Facilities			
(a) At **MARSEC Level 1**, in addition to the requirements of this part, an owner or operator of a barge fleeting facility must endure the implementation of the following security measures by:			
(1) Designating one or more restricted areas within the barge fleeting facility to handle those barges carrying, in bulk, cargoes regulated by 46 CFR Chapter I, subchapters D or O, or Certain Dangerous Cargoes;	☐	☐	☐
(2) Maintaining a current list of vessels and cargoes in the designated restricted area;	☐	☐	☐
(3) Ensuring that at least one towing vessel is available to service the fleeting facility for every 100 barges within the facility; and	☐	☐	☐
(4) Controlling access to the barges once tied to the fleeting area by implementing ***TWIC*** as described in 105.255 of this part.	☐	☐	☐
(b) At **MARSEC Level 2**, in addition to the requirements of this part and **MARSEC Level 1**, an owner or operator of a barge fleeting facility must ensure security personnel are assigned to monitor or patrol the designated restricted area within the barge fleeting facility.	☐	☐	☐
(d) At **MARSEC Level 3**, in addition to the requirements of this part and **MARSEC Level 2**, an owner or operator of a barge fleeting facility must ensure that both land and waterside perimeters of the designated restricted area within the barge fleeting facility are continuously monitored or patrolled.	☐	☐	☐

Sensitive Security Information (when filled out)

United States Coast Guard
FACILITY SECURITY PLANS (FSP) REVIEW CHECKLIST (General Facilities)

FIN: _____ ***Activity #:*** _____ ***Initials:*** _____ ***&*** _____

Item	***Explanation of Deficiency***

Comments

ENCLOSURE 4

SAMPLE PLAN REVIEW-RELATED LETTERS

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

Unit

Address
Staff Symbol:
Phone:
Fax:

Date
MISLE Activity # XXXXXXX FIN #: XXXXXX

Company Name
Attn:
Address
City, State, Zip

SAMPLE DENIAL LETTER

Dear *Mr./Ms./Captain XXXX*:

We have completed a review of your submitted Facility Security Plan (FSP) dated *[date]* for *[Facility Name]*. Unfortunately, your plan does not meet the requirements as outlined in 33 CFR Part 105. All deficiencies must be corrected and re-submitted to this office no later than 30 days from the date of this letter. Please note that **regulated operations cannot commence until final approval of the FSP by this office.** Enclosed, please find Enclosures (2) and (3) of NVIC 03-03 CH-2 to assist you in the preparation and review of your FSP prior to re-submittal.

Should you have any further questions concerning your facility security plan review, please contact *[title] [X. X. Name]* at [Telephone #].

Sincerely,

X. X. NAME
[title], U.S. Coast Guard
By direction

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

Unit

Address
Staff Symbol:
Phone:
Fax:

Date
MISLE Activity # XXXXXXX FIN #: XXXXXX

Company Name
Attn:
Address
City, State, Zip

SAMPLE PLAN APPROVAL LETTER

Dear *Mr./Ms./Captain 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 approved.

Commencing from the date of this letter, *[Facility Name]* must operate in compliance with this approved security plan and any additional requirements contained in 33 CFR Part 105. Your facility is subject to inspections at any time 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 FSP, 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 FSP is Sensitive Security Information and must be protected in accordance with 49 CFR Part 1520. A copy of your security plan and any amendments must be made available to Coast Guard personnel upon request.

This approval will remain valid until five years from the date of this letter unless rescinded in writing by this office. You must review your plans annually and submit any amendments to this office for re-approval as required by Title 33, CFR 105.410 and 105.415. **Keep a copy of this letter with the security plan.**

At a minimum, 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,

X. X. NAME
[title], U.S. Coast Guard
By direction

ENCLOSURE 5
ADDITIONAL APPLICABILITY GUIDANCE

5.1 Applicability Job Aid

5.1.1 The regulatory models indicated on the following pages are not intended to limit the discretion of the COTP. The COTP may depart from this guidance when expanding or reducing the regulated boundaries within a given facility, in order to prevent a Transportation Security Incident (TSI). Considerations such as the Area Maritime Security Plan (AMSP) may be taken into account by the COTP as well as provisions implemented by a facility that effectively mitigate vulnerabilities unique to that facility.

5.1.2 The requirements of 33 CFR 105.105 state the applicability for facilities. Once a facility owner/operator determines that the rule applies, and for the purposes of accurately identifying that portion of a facility's operation that is to be regulated under the rule, it is critical that close attention be given by plan submitters, reviewers and approvers when identifying exactly where a facility's maritime nexus begins and ends. In all cases, facility owners/operators, in accordance with the rule, their individual facility security assessments (FSA) and accepted security practices, are expected to effectively establish the physical boundaries of the facility's MTSA regulated area(s). This area(s) is to encompass only those aspects of operation that have, or in practicality cannot be functionally separated from, a maritime nexus. The FSP must mitigate the exploitation of FSA identified vulnerabilities, in the context of the maritime nexus, which could result in a Transportation Security Incident (TSI). COTPs are encouraged to closely consider how these regulated boundaries are determined by plan submitters in their review, approval, and/or denial of a Facility Security Plan (FSP); to ensure that the footprint of the regulated area(s) is neither too small nor too large. COTPs should be cautious when reviewing an FSP for approval or amendment that proposes a gross inclusion, expansion or shrinking of an MTSA regulated footprint, that does not meet the applicability standards given in 33 CFR 105.105.

5.1.3 For the purpose of illustration, in the singular case of marine transfer facilities (bulk oil and chemical facilities), under previous rules and regulations, the Coast Guard inspected to the first valve inside the secondary containment. The following scenarios are in keeping with this interpretation. The intent is to provide examples where consideration has been given in determining the maritime nexus as well as mechanisms that can be employed in establishing where that nexus begins and ends. Similar approaches may be taken by other industry owner/operators with regulated facilities. In all cases, the criteria employed in determining a facility's MTSA regulated boundary must be evident in its FSA wherein vulnerabilities, exploitable in the causation of a TSI, are identified and mitigated by the FSP.

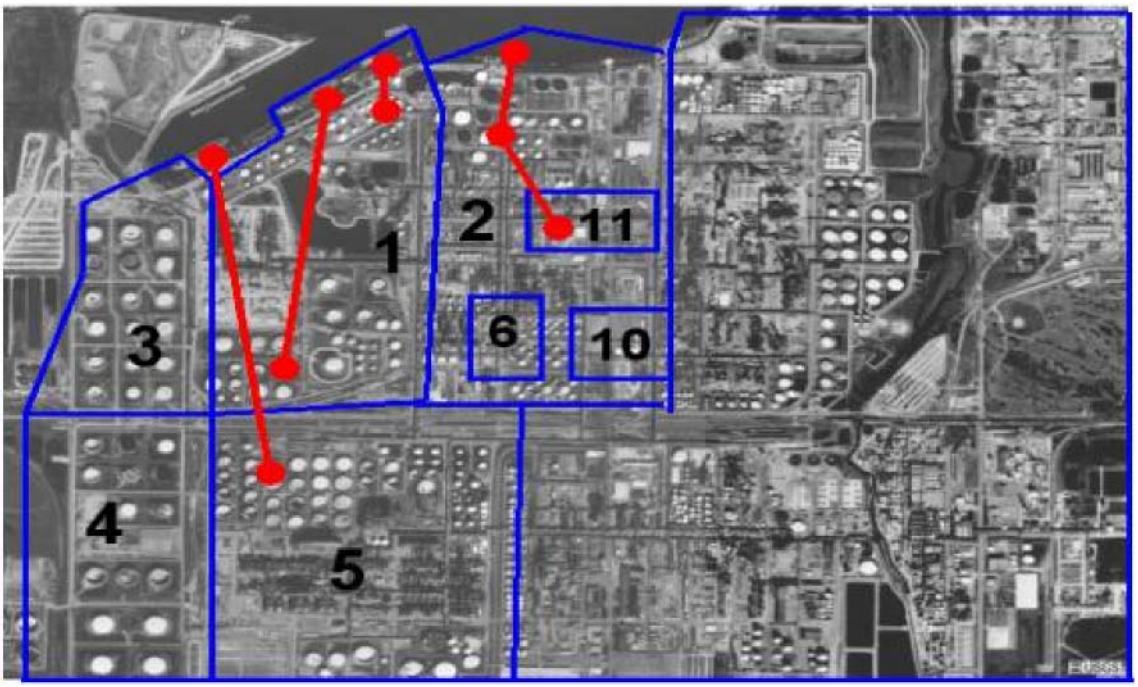
5.1.4 The COTP determines if a facility is isolated as defined in 33 CFR 105.105(c)(5). When making such a determination, the COTP should ensure that there is a lack of road access to the facility and that the facility does not distribute through secondary marine transfers. The COTP may wish to account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

Regulatory Application Models

Image 1

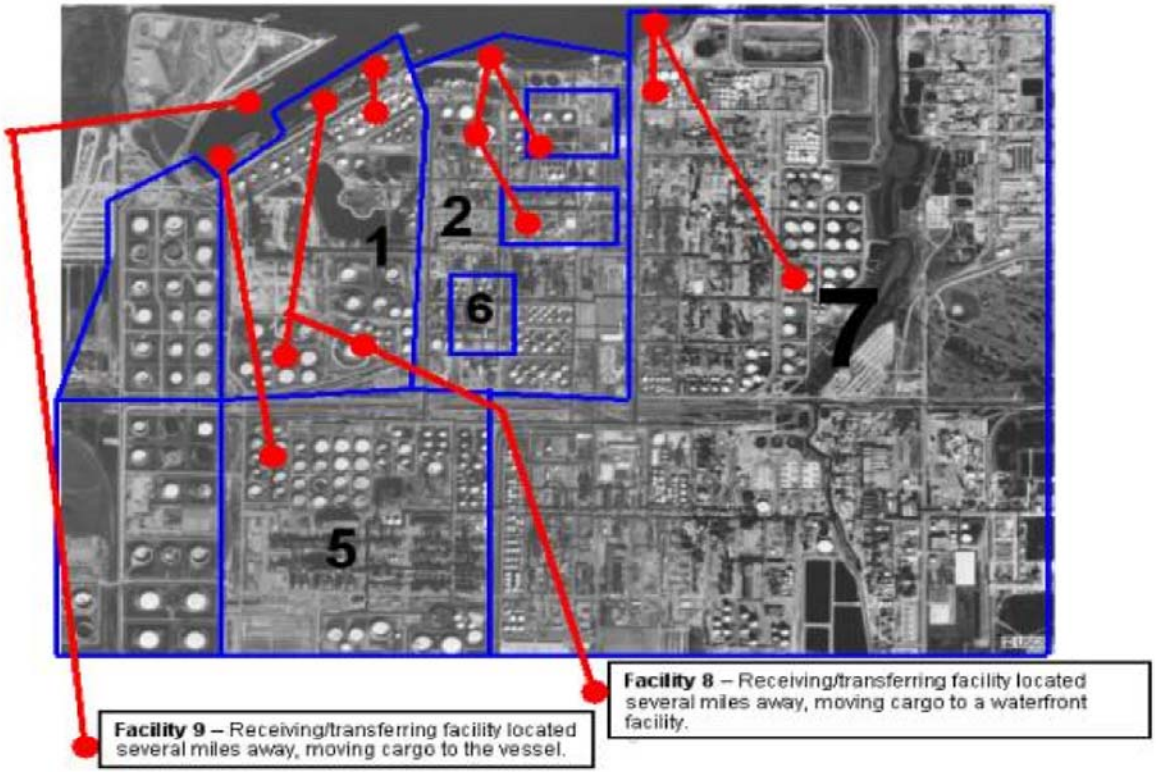
Scenario (Image 1)	Description	Regulated Area
1	A marine transportation-related (MTR) facility transferring cargo through a pipeline crosses a public street. However, the first valve within containment is located on the facility property across the street.	Both facility locations are regulated by 33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

Image 2



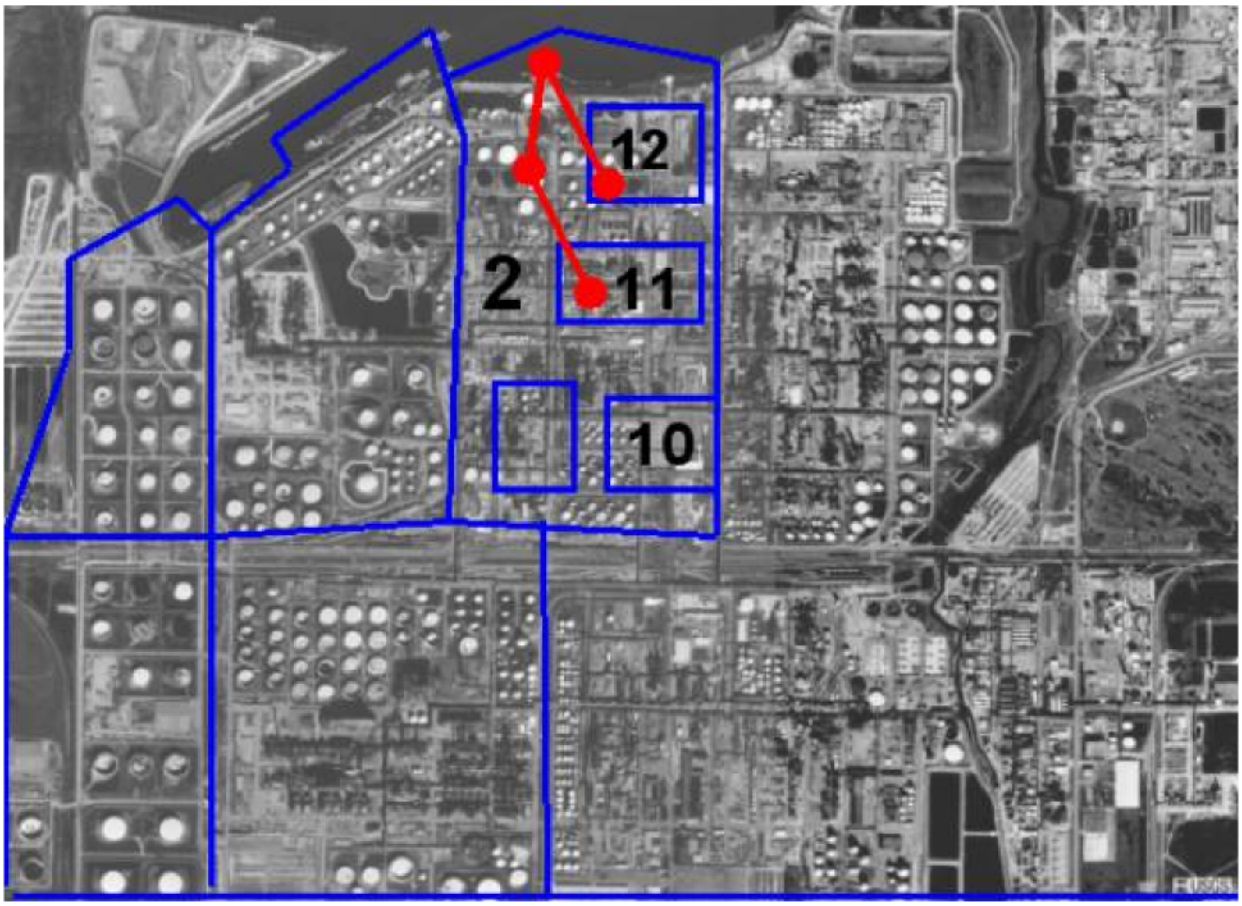
Scenario (Image 2)	Description	Regulated Area
3	**Facility 1** is located along the waterfront, transferring cargo to storage tanks adjacent to the waterfront, and to tanks within the manufacturing facility not adjacent to the waterfront.	**Facility 1** is regulated by 33 CFR 105. The vulnerability assessment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

Image 3



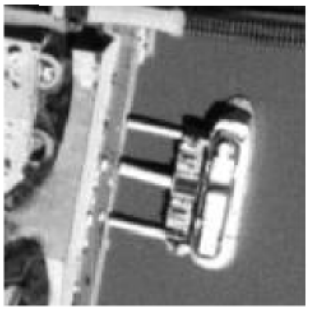
Scenario (Image 3)	Description	Regulated Area
7	**Facility 5** is not located on the waterfront itself, but it does have a MTR facility that transfers product back into the storage tanks within the facility. The "first valve within containment" is located near the tank farm area (not on the dock).	**Facility 5** is regulated and is required to be in compliance with 33 CFR 105. If the MTR facility has access control and is where the first valve within containment is located, Facility 5 would not be subject to 33 CFR 105.
8	**Facility 6** is located inside Facility 2, does not have any MTR activities, and is not located on the waterfront. Facility 2 must be entered in order to gain access to Facility 6..	**Facility 6** shall be accounted for in the Vulnerability Assessment and FSP of Facility 2. Facility 6 is not subject to 33 CFR 105.
9	**Facility 7** is similar to Facility 1, located along the waterfront, and transfers cargo to storage tanks adjacent to the waterway and to tanks within the production facility not adjacent to the waterfront.	**Facility 7** is required to be in compliance with 33 CFR 105. The plan will identify any restricted areas within the facility or consider the entire facility as a restricted area.
10	**Facility 8** is a separate company located several miles from the waterfront and transfers cargo to and from Facility 1, which transfers cargo to the MTR facility.	The transfer operation will be considered in the assessment for Facility 1. **Facility 8** is not subject to 33 CFR 105.
11	**Facility 9** transfers cargo through a pipeline from an MTR to a receiving/transferring facility located several miles away. The first valve within containment is located at the receiving/ transferring facility several miles from the waterfront.	**Facility 9** is regulated by 33 CFR 105. The plan will incorporate the marine facility, the pipeline, and the receiving facility.

Image 4



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

Image 5



Scenario (Image 5)	Description	Regulated Area
15	Facility in image 5 is a dock that has a casino boat permanently moored at the dock.	If the vessel is permanently moored and does not have a certificate of inspection, neither the vessel nor the facility will be regulated by 33 CFR 105.
16	A facility similar to the one in image 5 services cruise-type vessels that depart from the facility, sail up and down the river, and then returns to the same facility to disembark the passengers.	Both the vessel and facility are required to have separate plans. They can have a combined plan, but will have to submit it to both the MSC and COTP, and will have to have an index to cross-reference the vessel and facility requirements.
NOTE: *As of 31 Dec 2009, permanently moored vessels (i.e.: Casino) will no longer be MTSA regulated.*		
17	(No image provided) A ferry embarks and disembarks passengers and vehicles at two separate facilities.	The vessel and the facilities are required to be in compliance with 33 CFR 104 and 33 CFR 105. The separate plans may be consolidated into one. The consolidated plan will have to be submitted to both MSC (for vessels) and the local COTP (for the facilities). The consolidated plan will be cross-indexed for both vessels and facilities. The above situation refers to ferries that are not involved in coastwise or international voyages.
18	(No image provided) Facility receives a vessel on an ***international voyage*** carrying a non-hazardous material (e.g., rock, limestone, wood, timber) that calls on a manned/unmanned facility. In many cases, the vessel conducts the transfer operation with no shore assistance.	If the vessel exceeds 100 GRT, the facility must be in compliance with 33 CFR 105 and develop a facility security plan.
19	(No image provided) The same as scenario 18, but the vessel is only on a domestic voyage.	Same as scenario 18 except the facility is not required to be in compliance with 33 CFR 105 if it only receives domestic route vessels less than 100 GRT and does not receive certain dangerous cargoes (CDCs).

ENCLOSURE 6

SAMPLE DECLARATION OF SECURITY (DoS) DOCUMENT

Declaration of Security (DoS)
(Sample)

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

This *Declaration of Security* is valid from _____ until _____, for the following *facility/vessel* interface activities under MARSEC Level _____.

The facility and vessel agree to the following security responsibilities:

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

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

Date of issue: _____

_____	_____
(Signature of *Facility Security Officer)*	(Signature of *Master or Vessel Security Officer)*
_____	_____
(Name and Title, *Facility Security Officer)*	(Name and Title, *Master or Vessel Security Officer)*
Contact information: _____	Contact information: _____

ENCLOSURE 7

MTSA FACILITY COMPLIANCE GUIDE

USE OF THE MTSA FACILITY COMPLIANCE GUIDE

The Safe Port Act was signed by the President in October 2006 as part of ongoing efforts to develop countermeasures for traditional areas of vulnerability in the maritime domain. Among other things, this act modifies the provisions found in 46 USC 70103 by providing specific requirements for Coast Guard facility inspection performance. The Safe Port Act requires that the Coast Guard "verify the effectiveness of each facility security plan periodically, but not less than two times per year, at least one of which shall be an inspection of the facility that is conducted without notice to the facility."

To implement this requirement, the Coast Guard will conduct, within each 12 month period, a minimum of: (1) one announced annual MTSA Compliance Examination for each facility; (2) at least one unannounced Facility Security Spot Check for each facility; and, (3) where the Facility Security Spot Check or deficiency history warrants, an unannounced MTSA Compliance Examination.

At the Captain of the Port's (COTP) discretion, an unannounced Facility Security Spot Check may be expanded into a full, unannounced MTSA Compliance Examination.

Facility security spot checks performed under the MTSA facility inspection program will confirm facility compliance with the minimum performance-based security requirements in 33 CFR part 105. Facility security spot checks will, at a minimum:

A. Ensure that the security measures in place address vulnerabilities that were identified and documented on Form CG-6025 during the facility's vulnerability assessment;
B. Focus on traditional areas of national non-compliance such as security measures for restricted areas and access control;
C. Address past deficiencies based on the facility's security inspection history;
D. Confirm compliance with unique rules for facilities by type, such as screening standards required at cruise ship terminals;
E. Focus on implementation of the FSP (security awareness of employees, ability to execute security protocols, etc.);
F. Facility security spot checks should place less emphasis on items that do not change between annual MTSA facility compliance examinations (i.e., drills/exercise records); and,
G. Provide the facility with on-the-spot written documentation of both the results of the spot check and any security measures implemented by the facility to correct deficiencies noted.

This guide may be used for facility security spot checks. Security spot check items are marked "Spot Check" at the beginning of the inspection category. Items inspected for annual compliance exams but not typically inspected for security spot checks can be marked N/A for this purpose.

Units are encouraged to conduct multiple Security Spot Checks in accordance with the Maritime Security Risk Analysis Model (MSRAM) for facilities in their Area of Responsibility (AOR).

This guide is designed to assist Coast Guard inspectors in conducting field compliance inspections, to include Facility Security Spot Checks, of FSPs associated with 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 that key components of the MTSA regulations are verified.

This guide will also assist the Facility Security Officer and auditors [33 CFR 105.415(b)] in ongoing self-assessments of the facility security programs. There are four key steps that the Coast Guard inspector must follow when conducting a compliance inspection:

1) **Ensure** the completeness and adequacy of the Facility Security Assessment (FSA) and the Facility Vulnerability and Security Measures Summary (CG-6025)
2) **Ensure** the approved FSP/ASP adequately addresses the performance-based criteria as outlined in 33 CFR 105
3) **Ensure** that the measures in place adequately mitigate the vulnerabilities summarized on Form CG-6025.
4) **Ensure** the facility complies with the FSP

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, it cannot be used alone to verify that the facility has adequate security measures. The review of the FSA and FSP requires interaction with the facility owner, operator, designated security officers, and all personnel with related duties aboard the facility.

Pre-inspection Preparation	Inspection	Post-inspection Items
• Review FSA Report, Form CG-6025 and FSP • Review MISLE records • Review deficiency history • Review CG Activity History ***For Announced Inspections:*** • Schedule inspection with FSO and provide FSO with MTSA Facility Compliance Guide (Enclosure 7 of NVIC 03-03) with instructions for FSO to complete prior to Coast Guard inspection ***For Unannounced Facility Security Spot Checks:*** • Select the areas to be spot-checked and so indicate on the MTSA Facility Compliance Guide. (See pages 59 through 67 of this publication.)	• Verify FSA • Verify Form CG-6025 • Verify FSP implementation ***For Announced Inspections:*** • Complete and review the MTSA Facility Compliance Guide with the FSO ***For Unannounced Facility Security Spot Checks:*** • For unannounced (and full MTSA compliance exams), the inspector(s) shall select a time during the inspection, to confirm the availability of the FSO by contacting the FSO and advising him/her that an unannounced inspection is underway	• Complete MISLE *MTSA Compliance Exam* activity case • Determine whether amendments to the FSP are required • Initiate appropriate actions to ensure timely correction of deficiencies

Compliance inspections may address all or pre-selected areas of the MTSA regulations, and shall be done through observation of the current security procedures in place for each MARSEC Level; interviewing facility personnel regarding security duties and procedures; verifying on-site presence and validity of required security documents; and proper operation of security equipment. **This booklet is intended only as a guide to general MTSA requirements. Specific requirements will be contained in the FSP and implementing procedures.**

United States Coast Guard

MTSA FACILITY COMPLIANCE GUIDE

Name of Facility/Location:	**Facility Type:**
Facility ID Number:	**MISLE Activity Number:**
Inspection Type – Full or Spot Check:	**Areas Inspected: (ex. G-14, N-28-30 or All)**
Date(s) Conducted:	
Facility Security Officer Name:	**Date & Time FSO Contacted:**
Facility Inspectors: 1.	2.
3.	4.

Guidance for completing the *MTSA Facility Compliance Guide* (checklist) –
Coast Guard facility inspectors and facility security officers (FSOs) shall complete the checklist by verifying and, when applicable, demonstrating each item contained therein. Each inspected 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

FIN #_____ Inspector Initials and Date: _____

A. Compliance Documentation *33 CFR 105.120* **(Spot Check Item)**		SAT	N/O	N/A	FAIL
.120(a)	Approved Facility Security Plan (FSP), any approved revisions or amendments thereto, and Letter of Approval (LOA) from the COTP dated within the last 5 years;	☐	☐	☐	☐
.120(b)	FSP submitted for approval and an acknowledgement letter from COTP; ***OR***	☐	☐	☐	☐
.120(c)	An approved Alternative Security Program (ASP) as provided in 105.140: must have a copy of the ASP the facility is using, as specified in 101.120(b)(3) of this subchapter, and a letter signed by the facility owner or operator certifying the facility is in full compliance with that program.	☐	☐	☐	☐
	Note: Also **Review** the Facility Specific Security Assessment (FSA) report and CG-6025 for any changes or updates.	☐	☐	☐	☐

B. Non-Compliance *33 CFR 105.125* **(Spot Check Item)**	SAT	N/O	N/A	FAIL
.125 - Conditions existing (if any):				
1)_____	☐	☐	☐	☐
2)_____	☐	☐	☐	☐
- Conditions met?	☐	☐	☐	☐
- COTP notified of non-compliance?	☐	☐	☐	☐

C. Waivers & Equivalents *33 CFR 105.130 & 105.135* **(Spot Check Item)**		SAT	N/O	N/A	FAIL
.130	Approval letter for *Waiver(s)* from Commandant (CG-5442)	☐	☐	☐	☐
.135	Approval letter for *Equivalent(s)* from Commandant (CG-5442), as provided in 101.130 of this subchapter.	☐	☐	☐	☐

D. Maritime Security (MARSEC) Directives *33 CFR 105.145*		SAT	N/O	N/A	FAIL
.145	**Verify** the facility owner or operator has complied with and incorporated the instructions contained in a MARSEC Directive issued under 101.405 of this subchapter into the FSP.	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

E. Facility Security Officer (FSO) *33 CFR 105.205* **(Spot Check Item)**	SAT	N/O	N/A	FAIL
Name of FSO: _____ FSO Contact Information: Primary phone number: ( ) – Secondary phone number: ( ) –				
.205(a) General:				
(1) If the Facility Security Officer (FSO) performs other duties within the organization, **Verify** he or she is able to perform the duties and responsibilities required of the FSO.	☐	☐	☐	☐
(2) If the FSO serves more than one facility, **Verify** the facilities are in the same COTP zone, are not more than 50 miles apart, and the name of each facility is listed in the FSP.	☐	☐	☐	☐
(3) Verify if the FSO has assigned security duties to other facility personnel	☐	☐	☐	☐
(4) Verify the FSO has maintained a ***TWIC***.	☐	☐	☐	☐
.205(b) Qualifications:				
(1) **Verify** the FSO must have general knowledge through training or equivalent job experience, in the following:				
(i) Facility security organization;	☐	☐	☐	☐
(ii) General vessel and facility operations and conditions;	☐	☐	☐	☐
(iii) Vessel and facility security measures, including the meaning and the requirements of the different **MARSEC Levels**;	☐	☐	☐	☐
(iv) Emergency preparedness, response, and contingency planning;	☐	☐	☐	☐
(v) Security equipment and systems and their operational limitations; and	☐	☐	☐	☐
(vi) Methods of conducting audit, inspections, control, and monitoring techniques.	☐	☐	☐	☐
(2) **Verify** the FSO must have knowledge of and receive training in the following, as appropriate:				
(i) Relevant international laws and codes, and recommendations;	☐	☐	☐	☐
(ii) Relevant government legislation and regulations;	☐	☐	☐	☐
(iii) Responsibilities and functions of local, State, and Federal law enforcement agencies;	☐	☐	☐	☐
(iv) Security assessment methodology;	☐	☐	☐	☐
(v) Methods of facility security surveys and inspections;	☐	☐	☐	☐
(vi) Instruction techniques for security training and educations, including security measures and procedures;	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

E. Facility Security Officer (FSO) *33 CFR 105.205* **(Spot Check Item)**			SAT	N/O	N/A	FAIL
.205(b)(2) (con't)	(vii)	Handling sensitive security (SSI) information and security related communications;	☐	☐	☐	☐
	(viii)	Current security threats and patterns:	☐	☐	☐	☐
	(ix)	Recognizing and detecting dangerous substances and devices;	☐	☐	☐	☐
	(x)	Recognizing characteristics and behavioral patterns of persons who are likely to threaten security;	☐	☐	☐	☐
	(xi)	Techniques used to circumvent security measures;	☐	☐	☐	☐
	(xii)	Conducting physical searches and non-intrusive inspections;	☐	☐	☐	☐
	(xiii)	Conducting security drills and exercises, including exercises with vessels;	☐	☐	☐	☐
	(xiv)	Assessing security drills and exercises; and	☐	☐	☐	☐
	(xv)	Knowledge of ***TWIC*** requirements.	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

F. Facility Personnel With Security Duties **33 CFR 105.210** **(Spot Check Item)**		SAT	N/O	N/A	FAIL
.210	**Verify** that personnel **with security duties** are familiar with the FSP and relevant portions of the regulations. These personnel must have general knowledge through training or equivalent job experience in the following:				
.210(a)	Current security threats and patterns	☐	☐	☐	☐
,210(b)	Recognition and detection of dangerous substances and devices	☐	☐	☐	☐
.210(c)	Recognition of characteristics and behavioral patterns of persons who are likely to threaten security	☐	☐	☐	☐
.210(d)	Techniques used to circumvent security systems	☐	☐	☐	☐
.210(e)	Crowd management and control techniques	☐	☐	☐	☐
.210(f)	Security-related communications (including the handling of SSI)	☐	☐	☐	☐
.210(g)	Knowledge of emergency procedures and contingency plans	☐	☐	☐	☐
.210(h)	Operation of security equipment and systems	☐	☐	☐	☐
.210(i)	Testing, calibration, operation, and maintenance of security equipment and systems	☐	☐	☐	☐
.210(j)	Inspection, control, and monitoring techniques	☐	☐	☐	☐
.210(k)	Relevant provisions of the FSP	☐	☐	☐	☐
.210(l)	Methods of physical screening of persons, personal effects, baggage, cargo, and vessel stores	☐	☐	☐	☐
.210(m)	The meaning and the consequential requirements of the different MARSEC levels	☐	☐	☐	☐
.210(n)	Familiarity with all relevant aspects of the ***TWIC*** program and how to carry them out	☐	☐	☐	☐

G. Security Training for all other Facility Personnel **33 CFR 105.215** **(Spot Check Item)**		SAT	N/O	N/A	FAIL
.215	**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:				
.215(a)	Relevant provisions of the FSP & meaning of different MARSEC levels	☐	☐	☐	☐
.215(b)	Relevant meaning of the different MARSEC levels	☐	☐	☐	☐
.215(c)	Recognition & detection of dangerous substances and devices	☐	☐	☐	☐
.215(d)	Recognition of characteristics and behavioral patterns of persons who are likely to threaten security	☐	☐	☐	☐
.215(e)	Techniques used to circumvent security measures	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

G. Security Training for all other Facility Personnel **33 CFR 105.215** **(Spot Check Item)**	SAT	N/O	N/A	FAIL
.215(f) Familiarity with all relevant aspects of the ***TWIC*** program	☐	☐	☐	☐

H. Drill & Exercise Requirements **33 CFR 105.220**	SAT	N/O	N/A	FAIL
.220(a) *General:* (1) **Verify** the drills & exercises test the proficiency of facility personnel in assigned security duties at all MARSEC Levels and the effective implementation of the FSP.	☐	☐	☐	☐
(2) A drill or exercise required by this section may be satisfied with the implementation of security measures required by the FSP as the result of an increase in the MARSEC Level, provided the facility reports attainment to the cognizant COTP. *If so, Date/Type*: _____	☐	☐	☐	☐
.220(b) *Drills:* (1) **Review** Drill Log to ensure that at least one security drill is conducted every 3 months.	☐	☐	☐	☐
-Date/Type of last drill: _____				
(2) **Verify** the drills tested individual elements of the FSP, which included response to security threats and incidents.	☐	☐	☐	☐
.220(c) *Exercises:* (1) **Review** Exercise Log to ensure exercises are conducted at least once each calendar year, with no more than 18 months between exercises.	☐	☐	☐	☐
-Date/Type of last exercise: _____				
(2) **Note** which exercise(s) were used:				
(i) Full scale or live;	☐	☐	☐	☐
(ii) Tabletop simulation or seminar;	☐	☐	☐	☐
(iii) Combined with other appropriate exercise; or	☐	☐	☐	☐
(iv) Combination of elements in paragraphs (c)(2)(i) – (iii) of this section.	☐	☐	☐	☐

I. Facility Recordkeeping Requirements **33 CFR 105.225**	SAT	N/O	N/A	FAIL
.225(a) **Verify** the FSO has kept records of the activities for *at least 2 years* and makes them available to the Coast Guard upon request.	☐	☐	☐	☐
.225(b) **Review** records to ensure all of the following are recorded and protected accordingly (if kept in electronic format):				

FIN #_____ Inspector Initials and Date: _____

I. Facility Recordkeeping Requirements *33 CFR 105.225*		SAT	N/O	N/A	FAIL
	(1) Training records for facility personnel with security duties ONLY *(those personnel covered in 33 CFR 105.210)*	☐	☐	☐	☐
	(2) Drills and Exercises	☐	☐	☐	☐
	(3) Incidents and Breaches of Security	☐	☐	☐	☐
	(4) Change in MARSEC Levels	☐	☐	☐	☐
	(5) Maintenance, calibration, and testing of security equipment	☐	☐	☐	☐
	(6) Security Threats	☐	☐	☐	☐
	(7) Declaration of Security (DoS)	☐	☐	☐	☐
	(8) Annual audit of the FSP/ASP	☐	☐	☐	☐
	• **Verify** letter certified by the FSO states date the annual completed	☐	☐	☐	☐
	• **Verify** that past audit findings are addressed	☐	☐	☐	☐
.225(c)	**Verify** that the records required by this part are protected from unauthorized access or disclosure in accordance with SSI procedures	☐	☐	☐	☐

J. MARSEC Level Coordination and Implementation *33 CFR 105.230* **(Spot Check Item)**		SAT	N/O	N/A	FAIL
.230(a)	**Ensure** facility is operating at proper MARSEC level in effect for the Port, and **Review** procedures outlined in FSP for current MARSEC Level.	☐	☐	☐	☐
.230(b)	**Review** the procedures for changes in MARSEC levels:				
	(1) **Verify** notifications are made to vessels moored to or to arrive w/in 96 hours at facility of MARSEC change and the DoS is revised as necessary;	☐	☐	☐	☐
	(2) **Verify** facility complies with required additional security measures within 12 hours; and	☐	☐	☐	☐
	(3) **Verify** reports of compliance or non-compliance are made to the COTP.	☐	☐	☐	☐
.230(c)	**Review** procedures for **MARSEC Levels 2 & 3** that details how all facility personnel are informed about identified threats, and that emphasize reporting procedures/increased vigilance AS OUTLINED IN THE FSP.	☐	☐	☐	☐
.230(d)	**Ensure** the FSP has procedures in place if the facility is not in compliance with the requirements of this section such as informing the COTP and obtaining approval prior to vessel interface or continuing operations.	☐	☐	☐	☐
.230(f)	**Review** procedures for **MARSEC Level 3** that in addition to requirements of this part, the facility may be required to implement additional measure, pursuant to 33 CFR part 6, 160 or 165, as appropriate, which may include but are not limited to the following AS OUTLINED IN THE FSP:	☐	☐	☐	☐
	(1) Use of waterborne security patrol;	☐	☐	☐	☐
	(2) Use of armed security personnel to control access to the facility; and	☐	☐	☐	☐
	(3) Examination of piers, wharves and similar structures at the facility for the presence of dangerous substances, devices or other threats.	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

K. Communications *33 CFR 105.235*		SAT	N/O	N/A	FAIL
.235(a)	**Verify** the FSO has means to effectively notify personnel of changes of security conditions at the facility.	☐	☐	☐	☐
.235(b)	**Verify** that 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.	☐	☐	☐	☐
.235(c)	**Verify** that each active facility access point provides a means of contacting police, security control, or an emergency operations center.	☐	☐	☐	☐
.235(d)	**Verify** that the communications systems have a backup means for both internal and external communications.	☐	☐	☐	☐

L. Declaration of Security *33 CFR 105.225 and 105.245*		SAT	N/O	N/A	FAIL
.225(b)	(7) **Verify** that a copy of each single-visit DoS and a copy of each continuing DoS are kept with the FSP for at least 90 days after the end of its effective period.	☐	☐	☐	☐
.245(e)	**Verify** that at **MARSEC Level 1 & 2**, if the facility has implemented a continuing DoS, the FSO must *ensure* that:	☐	☐	☐	☐
	(1) The DoS is valid for a specific **MARSEC Level**	☐	☐	☐	☐
	(2) The effective period at **MARSEC Level 1** does not exceed 90 days	☐	☐	☐	☐
	(3) The effective period at **MARSEC Level 2** does not exceed 30 days	☐	☐	☐	☐
.245(f)	**Verify** the FSO is aware that when the MARSEC Level increases beyond that contained in a continuing DoS, it is then void, and a new DoS must be executed per this section.	☐	☐	☐	☐

M. Security Systems and Equipment Maintenance *33 CFR 105.250* **(Spot Check Item)**		SAT	N/O	N/A	FAIL
.250(a)	**Verify** that security systems and equipment are in good working order and inspected, tested, calibrated, and maintained according to manufacturers' recommendations.	☐	☐	☐	☐
.250(b)	**Verify** that security systems are regularly tested IAW the manufacturer's recommendations; noted deficiencies corrected promptly; and the results recorded as required by 105.225 of this subpart.	☐	☐	☐	☐
.250(c)	**Verify** the procedures used for identifying and responding to security and equipment failures or malfunctions.	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

N. Security Measures for Access Control 33 CFR 105.255 [and 105.257] (Spot Check Item)		SAT	N/O	N/A	FAIL
.255(f)	**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:	☐	☐	☐	☐
	(1) Demonstrate that the TWIC program is fully implemented and maintained;	☐	☐	☐	☐
	(2) Screen persons, baggage, personal effects, and vehicles, for dangerous substances and devices at the rate specified in the approved FSP;	☐	☐	☐	☐
	(3) Conspicuously post signs that describe security measures currently in effect and clearly state that: (i) Entering the facility is deemed valid consent to screening or inspection; and (ii) Failure to consent or submit to screening or inspection will result in denial or revocation of authorization to enter;	☐	☐	☐	☐
	(4) Check the identification of any person not holding a ***TWIC*** seeking to enter the facility, including vessel passengers and crew, vendors, government authorities, and visitors per means listed in .255(f)(4)(i)-(vi);	☐	☐	☐	☐
	(5) Deny or revoke a person's authorization to be on facility if the person is unable or unwilling to provide identity or account for his or her presence;	☐	☐	☐	☐
	(6) Designate restricted areas and provide appropriate access controls for these areas;	☐	☐	☐	☐
	(7) Identify access points that must be secured or attended to deter unauthorized access;	☐	☐	☐	☐
	(8) Deter unauthorized access to the facility and to designated restricted areas within the facility;	☐	☐	☐	☐
	(9) Screen by hand or device, such as x-ray, all unaccompanied baggage prior to loading onto a vessel; and	☐	☐	☐	☐
	(10) Secure unaccompanied baggage after screening in a designated restricted area and maintain security control during transfers between facility and vessel.	☐	☐	☐	☐
.255(g)	**Review** procedures for **MARSEC Level 2** to ensure that security measures relating to access control can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐
.255(h)	**Review** procedures for **MARSEC Level 3** to ensure that security measures relating to access control can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐

O. Security Measures for Newly-Hired Employees 33 CFR 105.257 (Spot Check Item)		SAT	N/O	N/A	FAIL
.257(a)-(b)&(d)	**Verify** that the facility owner or operator or the FSO ensures the implementation of the TWIC rules for all newly-hired employees in accordance with this section AS OUTLINED IN THE FSP.	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

O. Security Measures for Newly-Hired Employees 33 CFR 105.257 (Spot Check Item)		SAT	N/O	N/A	FAIL
.257(c)	**Verify** that the owner or operator acknowledges that this section does not apply to any person being hired as an FSO or any person being hired to perform facility security duties.	☐	☐	☐	☐

P. Security Measures for Restricted Areas 33 CFR 105.260 (Spot Check Item)		SAT	N/O	N/A	FAIL
.260(c)	**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:	☐	☐	☐	☐
	(1) Identify which facility personnel are authorized access;	☐	☐	☐	☐
	(2) Determine which persons other than facility personnel are authorized to have access;	☐	☐	☐	☐
	(3) Determine the conditions under which that access may take place;	☐	☐	☐	☐
	(4) Define the extent of any restricted area;	☐	☐	☐	☐
	(5) Define the times when access restrictions apply;	☐	☐	☐	☐
	(6) Clearly mark all restricted areas, indicating that access is restricted and that unauthorized presence within the area constitutes a breach of security;	☐	☐	☐	☐
	(7) Control the entry, parking, loading and unloading of vehicles;	☐	☐	☐	☐
	(8) Control the movement and storage of cargo and vessel stores; and	☐	☐	☐	☐
	(9) Control unaccompanied baggage or personnel effects.	☐	☐	☐	☐
.260(d)	**Verify** procedures at **MARSEC Level 1** to ensure that security measures relating to restricted areas are implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐
.260(e)	**Review** procedures for **MARSEC Level 2** to ensure that security measures relating to restricted areas can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐
.260(f)	**Review** procedures for **MARSEC Level 3** to ensure that security measures relating to restricted areas can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

Q. Security Measures for Handling Cargo *33 CFR 105.265* **(Spot Check Item)**		SAT	N/O	N/A	FAIL
.265(b)	**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:	☐	☐	☐	☐
	(1) Routinely check cargo, cargo transport units, and cargo storage areas within the facility prior to, and during, cargo handling operations for evidence of tampering;	☐	☐	☐	☐
	(2) Check that cargo, containers, or other cargo transport units entering the facility match the delivery note or equivalent cargo documentation;	☐	☐	☐	☐
	(3) Screen vehicles; and	☐	☐	☐	☐
	(4) Check seals and other methods used to prevent tampering upon entering the facility and upon storage within the facility.	☐	☐	☐	☐
.265(c)	**Review** procedures for **MARSEC Level 2** to ensure that security measures relating to handling of cargo can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐
.265(d)	**Review** procedures for **MARSEC Level 3** to ensure that security measures relating to handling of cargo can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐

R. Security Measures for Delivery of Vessel Stores and Bunkers *33 CFR 105.270* **(Spot Check Item)**		SAT	N/O	N/A	FAIL
.270(b)	**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:	☐	☐	☐	☐
	(1) Screen stores at rate specified in FSP	☐	☐	☐	☐
	(2) Require advance notification of vessel stores or bunkers delivery, including a list of stores, delivery vehicle driver and vehicle registration information;	☐	☐	☐	☐
	(3) Screen delivery vehicles at rate specified in FSP;	☐	☐	☐	☐
	(4) Escort delivery vehicles within the facility at rate specified in FSP.	☐	☐	☐	☐
.270(c)	**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.	☐	☐	☐	☐
.270(d)	**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.	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

S. Security Measures for Monitoring *33 CFR 105.275* **(Spot Check Item)**		SAT	N/O	N/A	FAIL
.275(b)	**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:				
	(1) When automatic intrusion-detection devices are used, that they activate an audible or visual alarm, or both, at a location that is continuously attended or monitored;	☐	☐	☐	☐
	(2) Is able to function continually, including consideration of the possible effects of weather or of a power disruption;	☐	☐	☐	☐
	(3) Monitors the facility area, including shore and waterside access to it;	☐	☐	☐	☐
	(4) Monitors access points, barriers and restricted areas;	☐	☐	☐	☐
	(5) Monitors access and movement adjacent to vessels using the facility, including augmentation of lighting provided by the vessel itself; and	☐	☐	☐	☐
	(6) Limits lighting effects, such as glare, and their impact on safety, navigation, and other security activities.	☐	☐	☐	☐
.275(c)	**Review** procedures for **MARSEC Level 2** to ensure that security measures relating to monitoring can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐
.275(d)	**Review** procedures for **MARSEC Level 3** to ensure that security measures relating to monitoring can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐

T. Security Incident Procedures *33 CFR 105.280*		SAT	N/O	N/A	FAIL
.280(a)	**Verify** procedures for responding to security threats or breaches of security and maintaining critical facility and vessel-to-facility interface.	☐	☐	☐	☐
.280(c)	**Review** procedures for reporting security incidents as required in 101.305 of this subchapter.	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

U. Passenger and Ferry Facilities Only ***33 CFR 105.285*** **(Spot Check Item)**		**SAT**	**N/O**	**N/A**	**FAIL**
.285(a)	**Verify** that at all **MARSEC Levels**, the facility ensures that the following security measures are implemented in addition to the requirements of this part:	☐	☐	☐	☐
	(1) Areas are established to segregate unchecked persons and effects from checked persons and effects;	☐	☐	☐	☐
	(2) A defined percentage of vehicles are being screened IAW the MARSEC Directive and FSP/ASP;	☐	☐	☐	☐
	(3) All unaccompanied vehicles to be loaded onto passenger vessels are screened prior to loading;	☐	☐	☐	☐
	(4) Security personnel control access to restricted areas; and	☐	☐	☐	☐
	(5) In a facility with a public access area designated under 105.106, provide sufficient security personnel to monitor all persons within the area.	☐	☐	☐	☐
.285(b)	**Review** procedures for **MARSEC Level 2** to ensure that security measures relating to passenger or ferry facilities can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐
.285(c)	**Review** procedures for **MARSEC Level 3** to ensure that security measures relating to passenger or ferry facilities can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐

V. Cruise Ship Terminals Only ***33 CFR 105.290*** **(Spot Check Item)**		**SAT**	**N/O**	**N/A**	**FAIL**
.290	**Verify** that at all **MARSEC Levels**, in coordination with the vessel moored at the facility, that the owner or operator has procedures that ensure the following security measures in addition to the requirements of this part:	☐	☐	☐	☐
.290(a)	Screening all persons, baggage, and all personal effects for dangerous substances and devices;	☐	☐	☐	☐
.290(b)	Checking personnel identification, including the applicable ***TWIC*** rules;	☐	☐	☐	☐
.290(c)	Designating holding, waiting, or embarkation areas to segregate screened persons and their personal effects;	☐	☐	☐	☐
.290(d)	Providing additional security personnel to designated holding, waiting, or embarkation areas within the facility's secure area; and	☐	☐	☐	☐
.290(e)	Denying individuals not holding a ***TWIC*** access to secure and restricted areas unless escorted.	☐	☐	☐	☐

FIN #_____ Inspector Initials and Date: _____

W. Certain Dangerous Cargo (CDC) Facilities Only *33 CFR 105.295* (Spot Check Item)		SAT	N/O	N/A	FAIL
.295(a)	**Verify** that at all **MARSEC Levels**, that the owner or operator of a CDC facility has procedures that ensure the implementation of the following security measures in addition to the requirements of this part:				
	(1) Escorting all visitors, contractors, vendors, and other non-facility employees;	☐	☐	☐	☐
	(2) Controlling parking, loading and unloading of vehicles within a facility;	☐	☐	☐	☐
	(3) Requiring security personnel to record or report their presence at key points during security patrols;	☐	☐	☐	☐
	(4) Searching key areas prior to vessel arrivals; and	☐	☐	☐	☐
	(5) Providing an alternate or independent power source for security and communications systems.	☐	☐	☐	☐
.295(b)	**Review** procedures for **MARSEC Level 2** to ensure that security measures relating to CDC facilities can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐
.295(c)	**Review** procedures for **MARSEC Level 3** to ensure that security measures relating to CDC facilities can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐

X. Barge Fleeting Facilities Only* *33 CFR 105.296* (Spot Check Item)		SAT	N/O	N/A	FAIL
.296(a)	**Verify** that at **MARSEC Level 1**, in addition to the requirements of this part, an owner or operator of a barge fleeting facility has procedures that ensure the implementation of the following security measures:				
	(1) Designating one or more restricted areas within the barge fleeting facility to handle those barges carrying, in bulk, cargoes regulated by 46 CFR chapter I, subchapters D or O, or Certain Dangerous Cargoes;	☐	☐	☐	☐
	(2) Maintaining a current list of vessels and cargoes in the designated restricted area;	☐	☐	☐	☐
	(3) Ensuring that at least one towing vessel is available to service the fleeting facility for every 100 barges within the facility;	☐	☐	☐	☐
	(4) Controlling access to the barges once tied to the fleeting area by implementing TWIC as described in 105.255 of this part.	☐	☐	☐	☐
.296(b)	**Review** procedures for **MARSEC Level 2** to ensure that security measures relating to barge fleeting facilities can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐
.296(c)	**Review** procedures for **MARSEC Level 3** to ensure that security measures relating to barge fleeting facilities can be implemented AS OUTLINED IN THE FSP.	☐	☐	☐	☐

**Barge fleeting facilities are exempt from Security Measures for Handling Cargo and Security Measures for Delivery of Vessel Stores and Bunkers*

FIN #_____ Inspector Initials and Date: _____

Notes on Deficiencies

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

1. *Facility is not operating in accordance with its approved/submitted FSP or ASP* – This type of deficiency is addressed utilizing a range of enforcement and compliance measures, from Lesser Administrative Actions (work lists, etc.), up to and including more significant measures such as Notice of Violations, Civil Penalties, and Operational Controls, which may restrict facility operations.
2. *Facility is operating in accordance with its approved/submitted FSP or ASP, but plan does not meet the specific performance criteria outlined in the regulations* – This type of deficiency 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 their 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:

- Facility personnel with security duties
- Facility personnel without security duties
- Facility recordkeeping requirements
- Communications
- Declaration of Security (DoS)
- Security systems and equipment maintenance
- Security measures for access control
- Security measures for newly-hired employees
- Security measures for restricted areas
- Security measures for handling cargo
- Security measures for delivery of vessel stores and bunkers
- Security measures for monitoring
- Security incident procedures

(Inspection Summary form included on next page)

FIN #_____ Inspector Initials and Date: _____

Inspection Summary

Discrepancy Description	*Cite*	*Corrective Action*	*Due Date*

Comments:

FIN #_____ Inspector Initials and Date: _____

ENCLOSURE 8

FACILITY SECURITY AUDITS

ENCLOSURE 8
FACILITY SECURITY AUDITS
Purpose:

A. Title 33, Part 101.105 (33 CFR 101.105) defines a*udit* as "an evaluation of a security assessment or security plan performed by an owner or operator, the owner or operator's designee, or an approved third party, ***intended to identify deficiencies, non-conformities, and/or inadequacies that would render the assessment or plan insufficient."*** 33 CFR 104.415, 105.415, and 106.415 provide requirements for the conduct of an annual audit of a regulated facility or vessel security plan. Owners and operators must ensure that audits are performed annually beginning no later than one year from the initial date of approval of their security plan with no more than18 months between audits.

B. The intent of the regulation and the purpose of an audit are to identify opportunities for improvement and to address non-conformities. An audit accomplishes this through the review of the operations of the regulated entity and the implementation of corrective actions which ensure regulatory compliance and preclude the recurrence of deficiencies. If, during the course of an audit, deficiencies and/or inadequacies are identified the security assessment and security plan of the regulated entity could have areas requiring improvement or revision. In this continuation of the audit and review of the security plans and assessments, more than one fix may need to be made. For instance, an identified security gap allowing unaccounted for persons to access a regulated entity would indicate a possible non-conformity in the implementation of the plan, or possibly point to deficiencies in the plan and/or assessment. It is the intent of the audit to make the security posture, and the underlying documentation, align and provide the tightest security appropriate for the situation.

C. Several opportunities exist for the auditor to analyze the effectiveness of the regulated entity in implementing their security plan. For example, review quarterly drills, annual exercises, and corrective action following a deficiency or recorded security event (such as a security incident or breach of security) provide an auditor the chance to see the plan operate and learn how it is improved. An effective audit might include site visits at the regulated facility or vessel during normal and other-than-normal hours, interviews with and observation of personnel performing security duties, review of and observation of security procedure implementation, as well as verifying operability testing and planned maintenance of security equipment, documentation, and performance verification of required training.

D. During the audit, several documents could assist the auditor in his or her duties. Such documents include those associated with previously performed audits, drills, exercises, security incidents, compliance inspections, corrective action reports, and lessons learned.

E. 33 CFR 105.225(b)(8) requires a letter certified by the Facility Security Officer stating the date the audit was completed. While there is no requirement that an audit report be maintained, the sample audit report form on the next page of this NVIC may be used by an auditor to help organize their thoughts and findings.

SAMPLE AUDIT REPORT FORM

REPORT NUMBER:

AUDIT DATE(S):

DATE OF LAST AUDIT:

AUDITORS AND EVIDENCE THEY MEET 33 CFR 104.415(b)(4) or 105.415(b)(4):

1.
2.
3.
4.
5.

EXECUTIVE SUMMARY:

This section gives the auditor the opportunity to briefly describe noteworthy findings (NF), observations (O), and Areas for Improvement (AFI).Note: Classification and Protection of Sensitive Security Information is found in 49 CFR Part 1520.

DEFICIENCIES, NON-CONFORMITIES, OR PLAN INADEQUACIES IDENTIFIED:

1.
2.
3.
4.
5.

STRENGTHS OF VESSEL OR FACILITY SECURITY:

This section gives the auditor the opportunity to briefly describe noteworthy findings (NF), observations (O), and Strengths.

NAME OF INVOLVED PARTIES FROM THE VESSEL OR THE FACILITY:

1.
2.
3.

Audit Report Prepared by: _____ Company: _____ Date: _____

Audit Report Reviewed by: _____ Position: _____ Date: _____

Audit Certification Letter Attached to VSP by: _____ Date: _____

ENCLOSURE (9)

GUIDANCE FOR SUBMISSION OF ALTERNATIVE SECURITY PROGRAM (ASP), EQUIVALENCY OR WAIVER REQUEST

9.1 Enclosure Contents

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

9.2 Guidance for submission of Alternative Security Program (ASP)
9.3 Application requirements
9.4 Program submission
9.5 Action upon receipt
9.6 Compliance
9.7 Operational security
9.8 Telephonic, e-mail and face-to-face inquiries
Figure 9-1-ASP Approval Process Flowchart
9.9 Guidance for submission of Equivalency Requests or Waiver Requests
9.10 Application requirements
9.11 Request submission
9.12 Action upon receipt
9.13 Operational Security
9.14 Telephonic, e-mail and face-to-face inquiries
Figure 9-2-Equivalency or Waiver Request Approval Process Flowchart

9.2 Guidance for submission of Alternative Security Programs (ASP)

9.2.1. The Final Rules published October 22, 2003 addressing the implementation of the Maritime Transportation Security Act of 2002 (MTSA) and the International Ship and Port Facility Security (ISPS) Code permits trade organizations or industry groups representing owners or operators to request approval for the use of an Alternative Security Program (ASP). The approved ASP must address all requirements in 33 CFR Parts 104, 105, or 106 as applicable. ASPs that will be used throughout a sector of the industry must be submitted and approved within a timeframe that allows owners or operators to choose between implementing the applicable ASP or implementing a security plan tailored to their specific vessel or facility.

9.3 Application requirements

9.3.1. ASPs that apply to an individual owner or operator must be submitted in accordance with 33 CFR 105.410 (a) and (b). Each ASP must contain:

1. A list of the vessel and/or facility types to which the ASP will apply.
2. A security assessment for the vessel and/or facility types.
3. An explanation of how the ASP addresses the requirements contained in 33 CFR Parts 104, 105, and/or 106, as applicable.
4. A specific explanation of how the owner and/or operator will implement each portion of the ASP. The ASP must explain which parts of the plan are applicable to various facilities, and require facility owners to activate/implement each part of the plan that applies to that type of facility.

5. We recommend including an index cross-referencing applicable sections of the regulations with the specific paragraphs or sections of the ASP.

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

9.4 Program submission

9.4.1. ASPs and any accompanying documents must be submitted via hard copy paper document, or a password protected copy may be placed on a floppy disc or compact disc (CD) in accordance with 33 CFR 105.410. ASPs shall not be submitted to the Coast Guard via e-mail, they must be mailed to:

COMMANDANT
(CG-54)
US COAST GUARD
2100 2nd ST SW
WASHINGTON DC 20593-0001

9.4.2. Each package must contain a:

- Point of contact
- Mailing address
- Telephone number

9.5 Action upon receipt

9.5.1. Applications will be reviewed in order of receipt.

9.5.2. Each application will undergo an initial review to ensure each required subject area is addressed. To pass initial review an ASP must meet qualifications requirements in 33 CFR 101.120, and must address all items of either 33 CFR 104.405 or 33 CFR 105.405 as appropriate. If the application is lacking critical information, it will be disapproved and the Coast Guard will send the submitter a letter containing a brief explanation of the reasons for disapproval. Coast Guard Headquarters COMDT (CG-54) will retain the application and related material for future reference.

9.5.3. Applications that pass the initial review will then undergo a detailed review. During this phase the ASP is reviewed to determine if it meets the intent of the entire rule for its specific industry type. The ASP content will be examined to determine compliance with all performance standards and at all MARSEC levels.

9.5.4. If the application is approved after the detailed review, a letter will be mailed to the submitter stating its acceptance and any conditions that may apply. Coast Guard Headquarters COMDT (CG-5442) will retain and file the application.

9.5.5. If the application is disapproved after the detailed review, a copy of the application will be returned to the submitter with a brief statement of the reasons for disapproval. The original

application will be kept on file at Coast Guard Headquarters COMDT (CG-54) for future reference. The organization will then have to make corrections and resubmit the program.

9.6 Compliance

9.6.1. Prior to conducting regulated operations, members using an ASP must do the following:

9.6.2. **Facility owners or operators** using an ASP must send their Facility Vulnerability Assessment CG-6025 to the Captain of the Port (COTP) along with a letter stating which approved ASP they are intending to use.

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

9.7 Operational security

9.7.1. Security plans, including Vessel Security Plans, Facility Security Plans, and ASPs, are considered Sensitive Security Information (SSI), and therefore, exempt from the Freedom of Information Act (FOIA), meaning that FOIA requests for ASPs will likely be denied. Any requests for such documents, however, should be forwarded to the applicable FOIA Officer and the CG-544 legal advisor for decision and action.

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

9.8.1. The regulations addressing security requirements are lengthy, complex, and vary in application from vessel to vessel, facility to facility, and port to port. Therefore, it is preferable that exchanges regarding regulation applicability take place in writing. Members of the public with specific applicability questions should submit their inquiries via letter or E-mail. Once the issue is properly researched, a written response will be provided. A list of Frequently Asked Questions (FAQs) and their answers will be posted on the USCG Port Security Directorate website at http://homeport.uscg.mil to assist the public. A MTSA/TWIC Help Desk has been established to assist the public with inquiries. The phone number for MTSA/TWIC Help Desk is 877-687-2243 and will be manned Monday through Friday from 0800 to 1600 hours Eastern Standard Time.

ALTERNATE SECURITY PROGRAM APPROVAL PROCESS

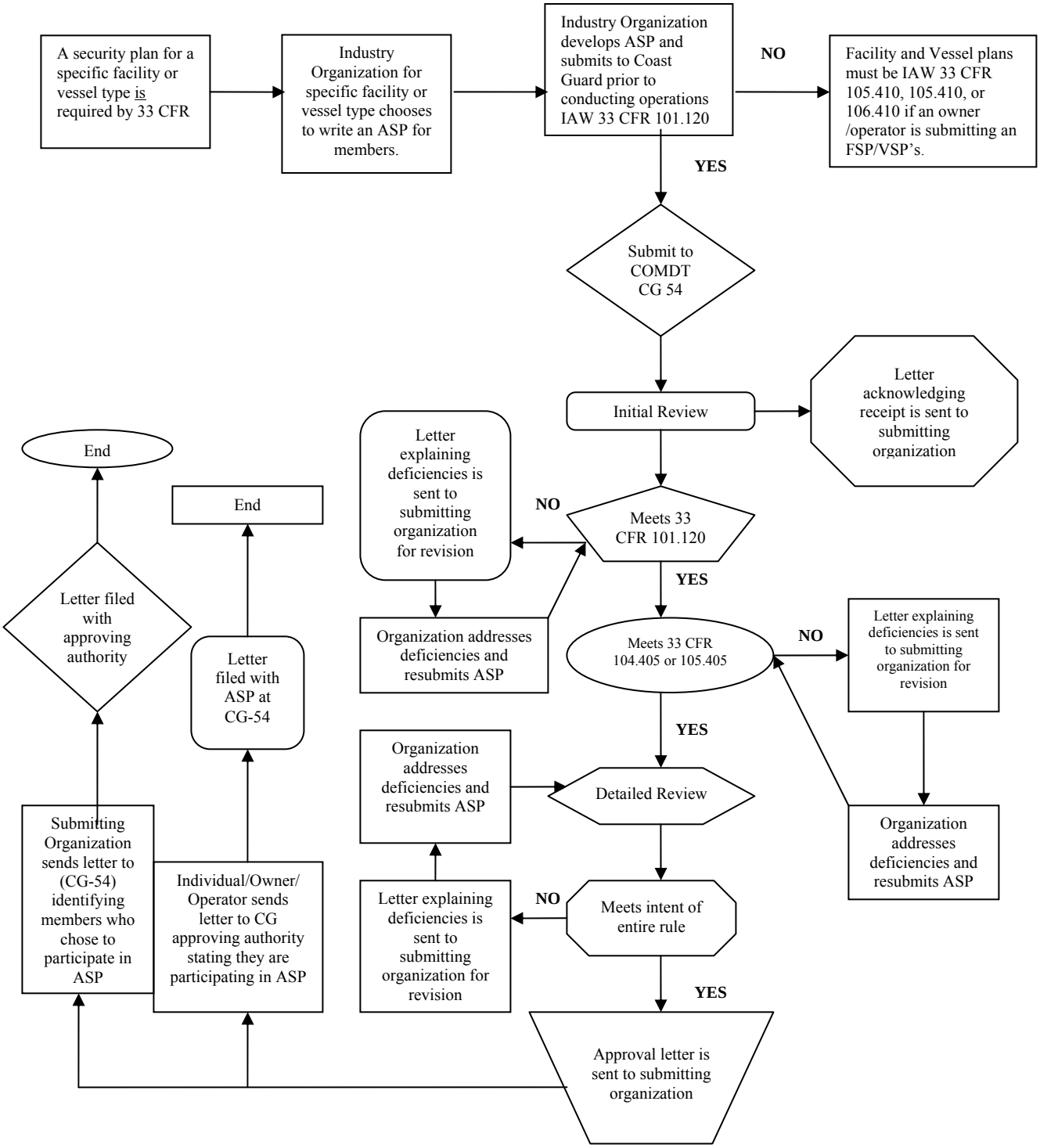


FIGURE 9-1

9.9 Guidance for submission of Equivalency Requests or Waiver Requests

9.9.1. The Final Rules published October 22, 2003 addressing the implementation of the Maritime Transportation Security Act of 2002 (MTSA) and the International Ship and Port Facility Security (ISPS) Code permits owners or operators to request approval for the use of Equivalent Security Measures (Equivalency Requests) or Waivers of Security Requirements (Waiver Requests).

9.10 Application requirements

9.10.1. Equivalency requests. For any security measure required by 33 CFR Parts 104, 105, or 106, the owner or operator may apply for approval to substitute an equivalent security measure that meets or exceeds the effectiveness of the required measure COMDT (CG-54) personnel will assess the adequacy of each equivalency request. Each application must contain:

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

9.10.2. Waiver requests. Owners or operators are permitted to apply for a waiver of any requirement in 33 CFR Parts 104, 105, or 106, that the owner or operator considers unnecessary in light of the nature or operating conditions of the vessel or facility COMDT (CG-54) personnel will assess the adequacy of each waiver request. Each application must contain:

1. The request for the waiver to a requirement.
2. The documentation supporting justification for the request.

9.11 Request submission

9.11.1 Equivalency and waiver requests along with any accompanying documents must be submitted via hard copy paper document, or a password protected copy may be placed on a floppy disc or compact disc (CD). Equivalency and waiver requests shall not be submitted to the Coast Guard via e-mail, they must be mailed to:

COMMANDANT
(CG-54)
US COAST GUARD
2100 2nd ST SW
WASHINGTON DC 20593-0001

9.11.2. Each package must contain a:

- Point of contact
- Mailing address
- Telephone number

9.12 Action upon receipt

9.12.1. Upon receipt a letter will be sent to the owner or operator from COMDT (CG-5442) acknowledging receipt of the equivalency or waiver request. In the letter the owner or operator will be directed to continue working on the facility or vessel security plan.

9.12.2. Applications will be reviewed in order of receipt.

9.12.3. Each application will undergo an initial review to ensure each required subject area is addressed. If the application is lacking critical information, it will be disapproved and the Coast Guard will send the submitter a letter containing a brief explanation of the reasons for disapproval. COMDT (CG-5442) will retain the application and related material for future reference.

9.12.4. Applications that pass the initial review will then undergo a detailed review. COMDT (CG-5442) may request further review and input from the Area commands. Atlantic Area and Pacific Area may disseminate for review as appropriate. All comments must be submitted to COMDT (CG-5442) within one week of Area receiving the request for input. During the detailed review, request content will be examined to determine compliance with the performance standards and at all MARSEC levels.

9.12.5. If the application is approved a letter will be mailed to the submitter stating its acceptance and any conditions that may apply. COMDT (CG-5442) will retain and file the application.

9.12.6. If the application is disapproved, a copy of the application will be returned to the submitter with a brief statement describing the reason for disapproval. The original application will be kept on file at COMDT (CG-5442) for future reference.

9.13 Operational Security

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

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

9.14.1. The regulations addressing security requirements are lengthy, complex, and vary in application from vessel to vessel, facility to facility, and port to port. Therefore, it is preferable that exchanges regarding regulation applicability take place in writing. Members of the public with specific applicability questions should submit their inquiries via letter or e-mail. Once the issue is properly researched, a written response will be provided. A list of Frequently Asked Questions (FAQs) with answers will be posted on the USCG Port Security Directorate website at http://homeport.uscg.mil to assist the public. A MTSA/TWIC Help Desk has been established to assist the public with inquiries.

EQUIVALENCY OR WAIVER REQUEST APPROVAL PROCESS

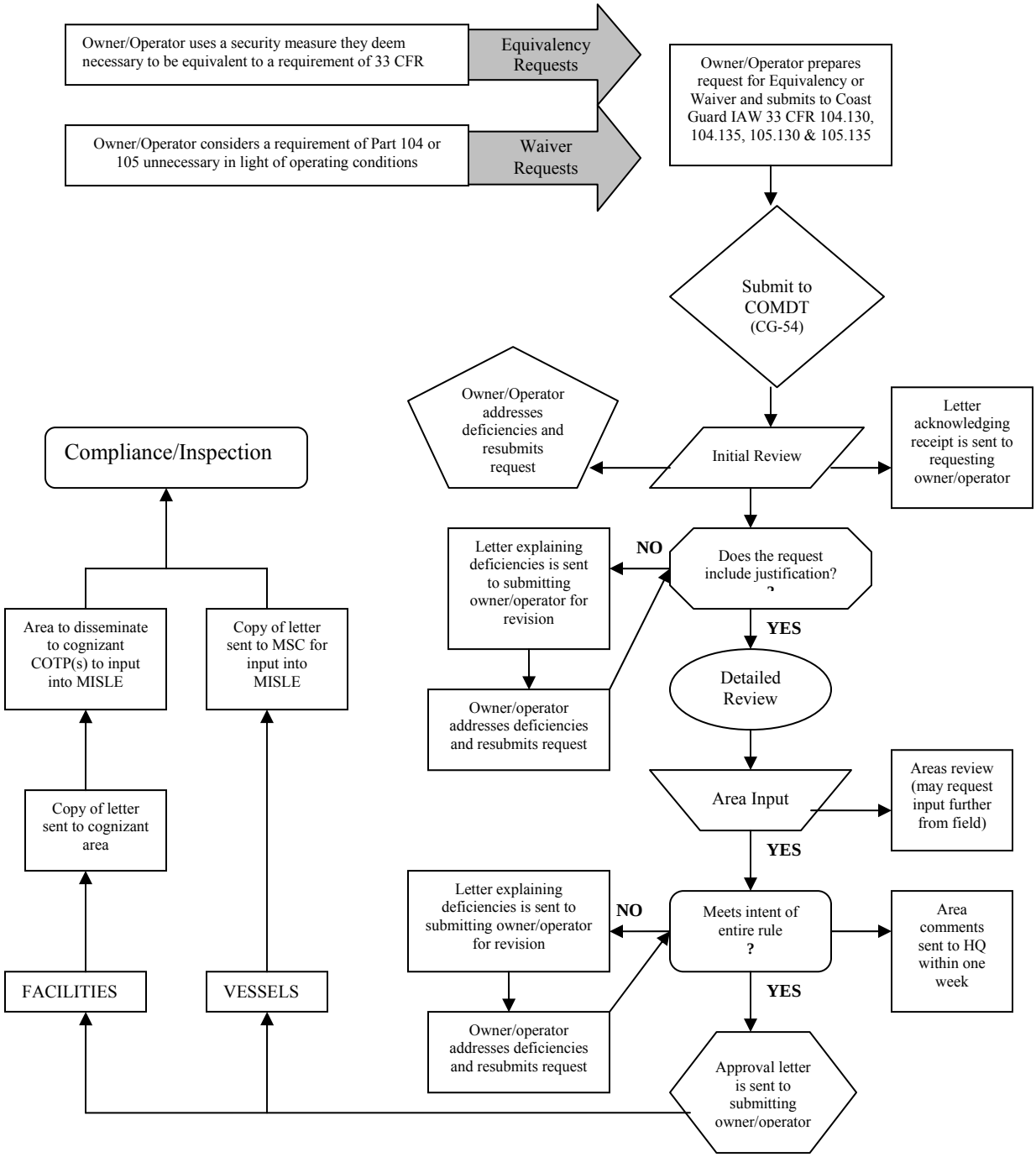


FIGURE 9-2

ENCLOSURE (10)

GUIDANCE FOR TRAINING STANDARDS AND AUDITING OF EXPLOSIVE DETECTION DOG TEAMS

RECOMMENDED EXPLOSIVES DETECTION DOG TEAM TRAINING STANDARDS

10.1 OVERVIEW.

10.1.1 Since the early 1990s, there have been various Scientific Working Groups (SWGs) initially sponsored by the FBI. SWGs are established to improve forensic science discipline practices and build consensus with international, federal, state, and local partners.

10.1.2 Currently several SWGs are active including the SWGDOG (Dog and Orthogonal Detector Guidelines). Though the primary goal of these SWGs is to develop guidelines to benefit local, state, federal and international law enforcement agencies in the performance and overall reliability of detector dogs, private entities are encouraged to use these as guidelines when choosing to use detector dogs as part of their Facility Security Plan.

10.2 INITIAL TRAINING OF EXPLOSIVES DETECTION DOG (EDD).

The following guidelines were developed in alignment with the SWGDOG criteria and are recommended for the initial training of explosive detection canines. When selecting a canine team for use at a cruise ship or ferry terminal, facility operators are encouraged to seek canine providers who meet these standards:

10.2.1 The canine training should:

1. Be conducted by a qualified explosives detector canine team trainer who is a competent individual from an organization that utilizes a structured curriculum with training designed to achieve specific learning objectives. A copy of the curriculum for the initial training course should be provided for review by the facility operator when considering the canine provider for security duties;

2. Include temperament, obedience, and search technique training. The handler must be able to demonstrate that the dog is non-aggressive and responds well to commands on and off leash. The canine should be able to be approached on and off leash without showing aggressive behavior. The team should be able to demonstrate proper search techniques including searching from as low as one foot to as high as eight feet;

3. Include dexterity/agility training. Dexterity training accustoms the dog to overcome physical obstructions encountered while executing a particular task. The dog is given the opportunity to become confident in climbing steep or unsteady areas and walk across uncomfortable surfaces such as iron grates. Dexterity exercises are also a means of instilling confidence in the dog that the handler will not command him to do anything that will result in injury. The EDD should be able to demonstrate the canine's dexterity in a variety of ways including a long jump, crawl exercise, directability at a distance, carrying and changing of dog handlers, etc;

4. Devote approximately half of the training hours in the initial training course to scent-

related tasks. These tasks include odor imprinting, tracking, and search activities including responding to scents hidden in a variety of locations;

5. Include training to detect the following mandatory groups of explosives that contain:

   (a) RDX (RDX based Detonation cord)
   (b) PETN (PETN (Pentrite) based Detonation cord)
   (c) TNT (Military TNT (Trinitrotoluene))
   (d) Dynamite (containing Ethylene Glycol Dinitrate (EGDN) and Nitroglycerin (NG))
   (e) Black powder (free flowing, time fuse or safety fuse)
   (f) Double base smokeless powder

6. Include other substances in the detection training as required by mission or specific threat. These substances may include:

   (a) Ammonium Nitrate (prilled or powder, or the solid component of binary explosives)
   (b) Black Powder substitutes (e.g., Pyrodex, Triple Seven)
   (c) Blasting Agents
   (d) Cast Boosters
   (e) Composition B
   (f) Emulsions
   (g) Nitromethane
   (h) Photoflash/fireworks/pyrotechnic powders
   (i) Plastic explosives (unmarked and marked with detection agent)
   (j) Semtex
   (k) Single Based smokeless powder
   (l) Slurries
   (m) Tetryl
   (n) Water gels
   (o) Home Made Explosives (HME)
      (i) Chlorate based mixtures (e.g., Potassium chlorate)
      (ii) Nitrate based mixtures (e.g., Anfo Nitrate)
      (iii) Perchlorate based mixtures (e.g., Potassium perchlorate)
      (iv) Urea nitrate
      (v) Peroxide based explosives
   (p) Hexamethylene Triperoxidediamine (HMTD)
   (q) Triacetone triperoxide (TATP)
   (r) Other emerging threats – Such as liquid explosives

7. Include varying quantities substances (dependent on region, mission and operational deployment needs);

8. Include exposing the canine to various heights and depths of training aid placement in different training scenarios;

9. Continue until the explosives detection canine is certified or deemed not certifiable by the standards used by the company, state or local law enforcement;

10.3 ADVANCED TRAINING OF EXPLOSIVES DETECTION DOG.

10.3.1 Maritime facilities offer a unique environment for explosives detection canine teams to operate. It is important that the canine receive advance training in the environment to which it is expected to perform. The following guidelines are recommended for the advanced training of explosives detection canines working in a marine environment. When selecting a canine team for use at a cruise ship or ferry terminal, facility operators are encouraged to seek canine providers who meet these standards:

10.3.2 Port Environment advanced training of EDD should include:

1. Familiarization with working in the port area;
2. Kenneling in the port environment;
3. First Aid - Protection of canines in harsh port conditions including chemicals;
4. Working in harness, lead, and off-lead;
5. Basic water training, including;
6. Canine familiarization to water;
7. Transfer from port to small craft;
8. Canine familiarization on small craft;
9. Transfer from small craft to port;
10. Transfer from small craft to larger craft;
11. Navigation on different surface types common in the port environment;
12. Working in and around food services;
13. Cross-training: searching pallets including stacked pallets using forklift;
14. Cross-training: searching cargo containers – internal and external;
15. Transferring on and off vessels using gangways;
16. Searching while on a moving vessel (ferry);
17. Advanced car search techniques - on and off ferry;
18. Avoiding distractions including other dogs in cars, loud noises, and passing boats;
19. Getting on board using alternative methods: harness, boat-to-boat, hoisting, carrying;
20. Distractions and instability: uneven seas and high noise levels;
21. Navigation on different types of flooring including metal floors;
22. Climbing ladders and stairways from one deck to another;
23. Facing various temperature controlled environments including humidity in cargo holds;
24. Baggage searching;
25. Vessel searching;
26. On-board cargo and or ships stores searching;

10.3.3 Advanced training may incorporate the integration of advanced technology that is currently used in facilities which includes:

1. Vapotrace equipment to identify explosive devices;
2. Radiation detectors;
3. X-ray machines;
4. Metal detection machines.

10.4 EVALUATION OF AN EXPLOSIVE DETECTION DOG TEAM

10.4.1 The following guidelines, again developed in alignment with SWGDOG criteria, are recommended for evaluating an explosives detection canine. When selecting a canine team for use at a cruise ship or ferry terminal, facility operators are encouraged to seek canine providers who meet these standards.

10.4.2 The EDD provider's certifying criteria for explosives detection dogs should be comprised of a comprehensive assessment that includes elements of odor recognition or double blind testing. Facility operators should be provided with a copy of the comprehensive assessment protocol employed by the training company or certifying organization.

10.4.3 Test Parameters;

1. The following parameters should be utilized during a canine certification process:

   (a) The explosives detector dog should be tested on the substance odors identified in 2(a) (5);
   (b) Recommended minimum quantities of substance odors for certification should be no less than ¼ lbs (113.5g);
   (c) Recommended optional substances are listed in 2(a) (6) and may be included in the test based on mission specific requirements;
   (d) As a minimum, the test shall include the following components:
      (i) Scenarios resembling searches within the normal operational environment;
      (ii) At least 4 different searches designed to evaluate the canine's ability to recognize the odor, respond to the odor and the handler's ability to recognize this response. Recommend the four different searches include;
         - Parcels/Baggage (for each explosive to be detected, testing material should be placed in 2-6 different parcels/bags. The average search time for 2-6 parcels/bags should be one minute);
         - Building/room search, of a 200 -1200 sq ft room with furniture (place one odor testing material per room. The average time should be 1.5 minutes or less to search 100 sq ft or 1000 cu ft);
         - Motor vehicles, both interiors and exteriors of passenger cars and trucks, using 2-6 vehicles per explosive testing odor. (Search time: 3 min per vehicle);

- Open area and perimeter searches of 1,000 to 10,000 sq ft for explosive test odor detection (Search time: 1-3 minutes per 1000 sq ft).

(iii) All odors for which the dog will be certified must be tested but not all odors will necessarily be in each type of search and some search areas shall contain no odors (blanks);
(iv) The recommended maximum time to complete an individual search is listed below but disqualification due to time shall be left to the discretion of the certifiers;
(v) The test shall end if the certifiers determine that the canine team is no longer working (e.g., Observable behaviors to be added).

(e) Minimum weight of substance being tested – ¼ pound (113.5 grams)
(f) Maximum weight of substance being tested - to be determined by the evaluator based on mission requirements and associated threat quantities
(g) Maximum height of hide – 8 ft
(h) Maximum depth of hide – 1 ft
(i) Minimum set time – 30 min or to be determined by the evaluator based on mission requirements and associated threat.
(j) The test should include a variety of searches designed to evaluate the canine's ability to recognize the odor, respond to the odor and the handler's ability to recognize this response.
(k) Training aids should not be placed in plain sight.
(l) The components built into the certification standards should include the following:
  (i) Positive Indication
  (ii) False Indication
  (iii) Non Indication (A non indicator is when the dog misses a hide)
  (iv) A team may fail as a result of excessive errors committed by the handler (inability to control the dog).
  (v) False response ratios should not exceed one response per ten items (i.e., bags, parcels) used in a certification. No more than two per operational search. (further refinement based on size of area)
(m) Use of distracters;
  (i) Natural distracters are normally present and vary depending on the area where the certification testing is done.
  (ii) Placement of distracters (distracters are other strong odors that may be present in the area of operation) in the certification area is required when no natural distracters are present.
  (iii) Care must be taken not to place artificial distractions in a manner that causes contamination with the test substance odor.
(n) Deliberate compromise of an evaluation should not be tolerated. Any communication (in person, by cell phone, two way pager, text messaging or by any other means) between handlers/department personnel participating in the evaluation, concerning specifics of an area still being evaluated, placement of explosives training aids or any information that could be regarded as a compromise prior to the termination (by the evaluator) will constitute a compromise of the

evaluation. In the event a handler compromises the evaluation, the handler should not be allowed to continue and may be removed from the evaluation.

10.5 MAINTENANCE TRAINING.

10.5.1 This type of training is meant to sustain and enhance the performance of the handler and canine and their ability to work together as a team. In maintenance training, situations are purposely sought where the capabilities of the canine team are challenged within the operational environments for which the team may be deployed.

10.5.2 The following guidelines based upon SWGDOG criteria are recommended for maintenance training of an explosives detection canine. When selecting a canine team for use at a cruise ship or ferry terminal, facility operators are encouraged to seek canine providers who meet these standards.

1. Maintenance Training shall include:

(a) A variety;
- (i) Of locations, environments and times of day
- (ii) Of training aid amounts and odors expected to be found within the operational environments
- (iii) Of heights, depths, containers and distraction odors
- (iv) Of types of searches (vehicles, building, parcels, luggage, open area)
- (v) In the duration of the searches
- (vi) Of blank searches

(b) The canine team should conduct regular objective-oriented training sessions sufficient to maintain operational proficiency.
- (i) Routine training, conducted solely by the handler to maintain the canine team's proficiency and to reinforce odor recognition, is an acceptable form of training but must be combined with supervised training on a regular basis. Supervised training conducted by a qualified trainer other than the handler, in order to improve performance, identify and correct training deficiencies and perform proficiency assessments is considered a best practice.
- (ii) A minimum of four hours per week should be spent in routine training for a canine team in order to maintain mission readiness.

(c) Maintenance training should represent all conditions that could be encountered during a certification process.

(d) Every effort shall be made to train during the initial training course with actual explosives and chemicals used in the making of explosives. Advanced training and maintenance training in a port environment shall require the use of "pseudo" instead of actual explosives due to security restrictions.

10.6 DOCUMENTATION.

10.6.1 The canine provider should maintain documentation that include all training records, training materials, proficiency assessments, seizure records, and/or deployment and utilization records of each canine. These records should be available to the facility owners for review.

10.6.2 The following guidelines based upon SWGDOG criteria are recommended for documentation of an explosive detection canine. When selecting a canine team for use at a cruise ship or ferry terminal, facility operators are encouraged to seek canine providers who meet these standards.

1. Records should contain discipline-related specifics.
2. Records should be standardized within the department, agency and/or organization.
3. Documents should be retained, in accordance with the Information and Life Cycle Management Manual COMDTINST M5212.12 (series). At minimum, records should be held for the length of the EDD Team contract. Records should contain but are not limited to the following:
4. Training records should include:

   (a) Date and time training took place
   (b) Name of trainer
   (c) Type and amount of training aid used
   (d) Length of training session
   (e) Location of training
   (f) Type of training (e.g., vehicle, luggage, building, open area)
   (g) Searches and indications

5. Certification records: (kept by Certifying authority and Handler)

   (a) Date certified
   (b) Certification authority i.e., agency, professional organization
   (c) Name of individual awarding certification
   (d) Type of materials for which certification granted
   (e) Location of certification
   (f) Name of canine and handler

6. Deployment/utilization:

   (a) Date and time
   (b) Location of deployment
   (c) Length of search
   (d) Description of activity
   (e) Results

7. Business documentation should include:

(a) Business License Number
(b) Kennel Business License Number, if applicable
(c) ATF License Number
(d) Insurance coverage (if required by licensing authority)
(e) Qualifications of Trainers and Handlers
(f) Handlers TWIC card information.

AUDITING EXPLOSIVES DETECTION DOG TEAMS

10.7 **OVERVIEW**. The purpose of this Appendix is to assist facility operators and MTSA facility auditors (Coast Guard) in the evaluation of EDDs when used at cruise ship or ferry operations. The Coast Guard's will in no way certify or accredit the EDD or EDD provider's training. The sole purpose of the Coast Guard's MTSA audit is to determine compliance of the approved facility security plan.

10.7.1 Facility operators and Coast Guard auditors are encouraged to use the following as a guide while evaluating Explosives Detection Dogs;

1. EXPLOSIVES DETECTION DOG PROVIDER BUSINESS INFORMATION.

   (a) Business Name and Address
   (b) Telephone and Fax Numbers
   (c) Business License Number (Standard: The firm must be registered to do business in its state(s) of operations).
   (d) Kennel Business License Number (Standard: If the firm maintains a kennel operation, its license must be current and permit the number of kennels on its property.)
   (e) ATF License Number if not using ATF approved "pseudos." ("Pseudos" are sometimes used in training explosive dogs when "real" explosives cannot be used. It is important that pseudos are ATF approved to validate their effectiveness in training and testing. Pseudos are commonly used in remote training scenarios including the port and ferry locations involved with this program.)
   (f) Qualifications of Trainers**;** Provide evidence of training experience. Where did the trainers learn how to train dogs? For example; do they have military or police canine experience?
   (g) Curriculum and methods; upon request, make available a detailed, week-by-week lesson plan for the provider's explosives scent detection training program.

2. EXPLOSIVES DETECTION DOG TEAM INFORMATION

   (a) Review of TWIC for each team member: (Team primary responsibility is facility security, therefore a valid TWIC is required).
   (b) Review of Records of training, certification testing, and canine health for each dog used on the facility.
   (c) Review of Records of training for each handler used on the facility.
   (d) Kennel evaluation for cleanliness and environment protection (if kennel location is provided on the facility, the canines living conditions should be evaluated).

3. PASSIVE OBERSERVATIONS OF THE EXPLOSIVES DETECTION DOG OPERATIONS;

   (a) Ability of the dog getting on and off vessels as necessary (navigation of gangways or

brow).

(b) Car search ability, if required.
(c) Ability not to be distracted by other dogs, vehicles, loud noises, and passing boats or people.
(d) Ability to search baggage (handheld and checked)
(e) Ability to search ship stores and/or cargo.
(f) Does dog display shyness, aggressiveness, jump up on people or react in any way that would be construed as poor or weak temperament.
(g) Does the dog handler have the ability to control the canine while working (is the dog obedient to the handler's commands).

10.7.2 Required security drills and exercises are good opportunities to observe EDD operations. Facility operators and Coast Guard auditors are encouraged to include EDDs in drill and exercise scenarios. The following tests are recommendations for inclusion in drill and exercise scenarios. Coast Guard auditors should only observe the scenarios and not be participants.

1. Exercise to evaluate the EDDs temperament may include the following;

(a) The dog walking over various surfaces found in its working environment (grating, cement, tile etc)
(b) A can of stones will be tossed out in front of the dog from a person out of sight
(c) A person carrying an umbrella pass by and suddenly open the umbrella in the vicinity of the dog, but without making direct contact.
(d) Several persons pass both in front towards the dog and from behind.
(e) The EDD and handler is to walk through a group of people in the working environment.
(f) A vehicle approaching from the front, but not directly in the path of the team and blow the horn several times.
(g) Another dog passing in the vicinity of the team, whereby the dog may react to some degree, but must remain under the control of the handler at all times. A dog that shows excessive aggression or total submissiveness cannot pass.
(h) During this test, at no time may the dog display shyness, aggressiveness, jump up on people or react in any way that would be construed as poor or weak temperament.

2. Exercise to evaluate the EDDs obedience may include the following;

(a) Heeling on Leash (The dog and handler demonstrates in a normal stride 30 paces in straight line work with an about turn into the dog. After 5 paces the handler commands the dog to move fast for 5 paces, then show 5 paces slowly and then move forward at a normal stride.
(b) Group Work – off leash. The purpose of the phase of obedience is to demonstrate control of the dog in any environment. The handler should wear appropriate attire, such as his/her uniform, sports outfit, etc., and may not carry any toys, balls, food as a support tool during the test. The dog will enter the group of 3 to 5 people and weave through the group passing by each person. It will conclude with the handler halting

near any person.

(c) Heeling off Leash (The dog and handler demonstrates the same pattern as outlined under b(1) as an off leash exercise).

(d) Sit in Motion (After a development of 10 to 15 paces, the dog is commanded to "sit" and he/she must assume this position quickly and without hesitation. The handler should then precede another 20 paces and then turn facing the dog. After a moment the handler will return to the dog's position).

(e) Down in Motion. (After a development of 10 to 15 paces, the handler commands the dog "down". The dog must assume this position quickly and without hesitation. The handler then proceeds another 20 paces and then turn facing the dog. After a moment the handler will return to the dog's position).

(f) Down with recall. (After a development of 10 to 15 paces, the dog handler will command "down". The dog must assume this position quickly and without hesitation. The handler then precedes 30 paces and turns to face the dog. The handler then recalls the dog to him.

(g) Send Away. (After a development of approximately 10 to 15 paces, the dog is dispatched to go out approximately 30 paces and then commanded to down. The dog is to go out quickly and be goal oriented and down immediately upon command).

3. Exercise to evaluate the EDDs ability to detect explosives may include the following;

(a) Single hit area search. (Direct the placement of explosive test material test in a single piece of luggage within the EDDs working environment (facility/vessel) with a group of 5 or more other luggage pieces placed around, on top of or stacked under the test luggage. The EDD Team should not be present when placing the test material).

(b) Multiple hit search. (Direct the placement of explosive test material in three different areas of the EDDs working environment (facility/vessel). Explosive test material should be placed at different heights. The EDD Team should not be present when placing the test material).

(c) Single vehicle search. (Direct the placement of explosive test material in a vehicle within the EDDs working environment. The EDD Team should not be present when placing the test material.

(d) Multiple vehicle searches. (Direct the placement of explosive test material in three different vehicles of a possible 8 vehicles which will enter or are present in the EDDs working environment. Explosive test material should be placed at different heights. The EDD Team should not be present when placing the test material).

ENCLOSURE 11

USCG FACILITY SECURITY SPOT CHECK GUIDE

Sensitive Security Information *(when filled out)*

USCG FACILITY SECURITY SPOT CHECK GUIDE

Facility: _____ *FIN:* _____ *Activity #:*_____

*Date Conducted:*_____ *CG Team:* _____ & _____

Requirements as per *33 CFR Subchapter H* *(Suggestions for SSCs; may use some or all)*	***Cite***	**SAT**	**N/O**	**N/A**	**FAIL**
Compliance Documentation – (Are the FSP/ASP/LOA up to date, any revisions made)	105.210	☐	☐	☐	☐
Non-Compliance – (Any conditions)	105.125	☐	☐	☐	☐
Waivers & Equivalents – (Any approval letters)	105.130 105.135	☐	☐	☐	☐
Facility Owner or Operator – (Any changes to key personnel)	105.200	☐	☐	☐	☐
Facility Security Officer – (Any changes, maintained a TWIC)	105.205	☐	☐	☐	☐
Facility Personnel with Security Duties – (Have TWIC, knowledge of duties)	105.210	☐	☐	☐	☐
Security Training for all other Facility Personnel – (Familiar with TWIC, relevant provisions of FSP & MARSEC Levels)	105.215	☐	☐	☐	☐
MARSEC Level Coordination & Implementation – (i.e.: Facility at proper MARSEC Level & posted)	105.230	☐	☐	☐	☐
Communications – (Access point security has ability to notify in event of emergency)	105.235	☐	☐	☐	☐
Security Systems and Equipment Maintenance – (Good working order; inspected / repaired per manufacturer's recommendations)	105.250	☐	☐	☐	☐
Access Control – (Access points identified, I.D. checks, screening baggage, personal effects, vehicles, securing unaccompanied baggage, signs posted, TWIC compliant)	105.255 *(101.515)*	☐	☐	☐	☐
Newly-Hired Employees – (New employees have or in process of having a TWIC & knowledge of TWIC program)	105.257	☐	☐	☐	☐
Restricted Areas – (Identified / clearly marked, control entry and movement of vehicles, storage of cargo & stores, unaccompanied baggage or personnel effects)	105.260	☐	☐	☐	☐
Cargo Handling – (Check cargo, storage areas prior to/during ops, compare cargo with delivery documentation, check seal/methods to prevent tampering)	105.265	☐	☐	☐	☐

Sensitive Security Information *(when filled out)*

USCG FACILITY SECURITY SPOT CHECK GUIDE

Requirements as per *33 CFR Subchapter H* *Suggestions for SSC's, may use all or some)*	***Cite***	**SAT**	**N/O**	**N/A**	**FAIL**
Vessel Stores/Bunkers – (Screening stores and vehicles at rates specified and advance notice of deliveries?)	105.270	☐	☐	☐	☐
Monitoring – (Facility area, shore/waterside access; restricted areas; vessel/area surrounding vessel?)	105.275	☐	☐	☐	☐
Additional Requirements – Passenger and Ferry Facilities	105.285	☐	☐	☐	☐
Additional Requirements – Cruise Ship Terminals	105.290	☐	☐	☐	☐
Additional Requirements – Certain Dangerous Cargo (CDC) Facilities	105.295	☐	☐	☐	☐
Additional Requirements – Barge Fleeting Facilities	105.296	☐	☐	☐	☐

SAT *– Satisfactory* ***N/O*** *– Not Observed* ***N/A*** *– Not Applicable* ***FAIL*** *– Item Failed Inspection*

Discrepancy Description	***Cite***	***Corrective Action***	***Due Date***

Comments:

USCG Inspector

(Printed Name)

(Signature)

Facility Security Officer

(Printed Name)

(Signature)