

- (3) Drills and exercises;
- (4) Records and documentation;
- (5) Response to change in MARSEC Level;
- (6) Procedures for interfacing with vessels;
- (7) Declaration of Security (DoS);
- (8) Communications;
- (9) Security systems and equipment maintenance;
- (10) Security measures for access control, including designated public access areas;
- (11) Security measures for restricted areas;
- (12) Security measures for handling cargo;
- (13) Security measures for delivery of vessel stores and bunkers;
- (14) Security measures for monitoring;
- (15) Security incident procedures;
- (16) Audits and security plan amendments;
- (17) Facility Security Assessment (FSA) report; and
- (18) Facility Vulnerability and Security Measures Summary (Form CG-6025) in appendix A to part 105—Facility Vulnerability and Security Measures Summary (CG-6025).

(b) The facility owner or operator must ensure that the FSP describes in detail how each of the individual requirements of subpart B of this part will be met.

(c) The Facility Vulnerability and Security Measures Summary (Form CG-6025) must be completed using information in the FSA concerning identified vulnerabilities and information in the FSP concerning security measures in mitigation of these vulnerabilities.

§ 105.410 Submission and approval.

(a) On or before December 31, 2003, the owner or operator of each facility currently in operation must either:

- (1) Submit one copy of their Facility Security Plan (FSP) for review and approval to the cognizant COTP and a letter certifying that the FSP meets applicable requirements of this part; or
- (2) If intending to operate under an Approved Security Program, a letter signed by the facility owner or operator stating which approved Alter-

native Security Program the owner or operator intends to use.

(b) Owners or operators of facilities not in service on or before December 31, 2003, must comply with the requirements in paragraph (a) of this section 60 days prior to beginning operations or by December 31, 2003, whichever is later.

(c) The cognizant COTP will examine each submission for compliance with this part and either:

(1) Approve it and specify any conditions of approval, returning to the submitter a letter stating its acceptance and any conditions;

(2) Return it for revision, returning a copy to the submitter with brief descriptions of the required revisions; or

(3) Disapprove it, returning a copy to the submitter with a brief statement of the reasons for disapproval.

(d) An FSP may be submitted and approved to cover more than one facility where they share similarities in design and operations, if authorized and approved by each cognizant COTP.

(e) Each facility owner or operator that submits one FSP to cover two or more facilities of similar design and operation must address facility-specific information that includes the design and operational characteristics of each facility and must complete a separate Facility Vulnerability and Security Measures Summary (Form CG-6025), in appendix A to part 105—Facility Vulnerability and Security Measures Summary (CG-6025), for each facility covered by the plan.

(f) A FSP that is approved by the cognizant COTP is valid for five years from the date of its approval.

[USCG-2003-14732, 68 FR 39322, July 1, 2003; 68 FR 41916, July 16, 2003, as amended at 68 FR 60542, Oct. 22, 2003]

§ 105.415 Amendment and audit.

(a) *Amendments.* (1) Amendments to a Facility Security Plan (FSP) that is approved by the cognizant COTP may be initiated by:

- (i) The facility owner or operator; or
- (ii) The cognizant COTP upon a determination that an amendment is needed to maintain the facility's security. The cognizant COTP, who will give the facility owner or operator

written notice and request that the facility owner or operator propose amendments addressing any matters specified in the notice. The facility owner or operator will have at least 60 days to submit its proposed amendments. Until amendments are approved, the facility owner or operator shall ensure temporary security measures are implemented to the satisfaction of the COTP.

(2) Proposed amendments must be submitted to the cognizant COTP. If initiated by the facility owner or operator, the proposed amendment must be submitted at least 30 days before the amendment is to take effect unless the cognizant COTP allows a shorter period. The cognizant COTP will approve or disapprove the proposed amendment in accordance with § 105.410 of this subpart.

(3) Nothing in this section should be construed as limiting the facility owner or operator from the timely implementation of such additional security measures not enumerated in the approved FSP as necessary to address exigent security situations. In such cases, the owner or operator must notify the cognizant COTP by the most rapid means practicable as to the nature of the additional measures, the circumstances that prompted these additional measures, and the period of time these additional measures are expected to be in place.

(4) If there is a change in the owner or operator, the Facility Security Officer (FSO) must amend the FSP to include the name and contact information of the new facility owner or operator and submit the affected portion of the FSP for review and approval in accordance with § 105.410 if this subpart.

(b) *Audits.* (1) The FSO must ensure an audit of the FSP is performed annually, beginning no later than one year from the initial date of approval, and attach a letter to the FSP certifying that the FSP meets the applicable requirements of this part.

(2) The FSP must be audited if there is a change in the facility's ownership or operator, or if there have been modifications to the facility, including but not limited to physical structure, emergency response procedures, security measures, or operations.

(3) Auditing the FSP as a result of modifications to the facility may be limited to those sections of the FSP affected by the facility modifications.

(4) Unless impracticable due to the size and nature of the company or the facility, personnel conducting internal audits of the security measures specified in the FSP or evaluating its implementation must:

(i) Have knowledge of methods for conducting audits and inspections, and security, control, and monitoring techniques;

(ii) Not have regularly assigned security duties; and

(iii) Be independent of any security measures being audited.

(5) If the results of an audit require amendment of either the FSA or FSP, the FSO must submit, in accordance with § 105.410 of this subpart, the amendments to the cognizant COTP for review and approval no later than 30 days after completion of the audit and a letter certifying that the amended FSP meets the applicable requirements of this part.

[USCG-2003-14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60542, Oct. 22, 2003]

APPENDIX A TO PART 105—FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY (FORM CG-6025)

U.S. DEPARTMENT OF HOMELAND SECURITY U.S. COAST GUARD CG-6025 (05/03)		FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY		OMB APPROVAL NO. 1625-0077
An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The Coast Guard estimates that the average burden for this report is 60 minutes. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: Commandant (G-MP), U.S. Coast Guard, 2100 2nd St, SW, Washington D.C. 20593-0001 or Office of Management and Budget, Paperwork Reduction Project (1625-0077), Washington, DC 20503.				
FACILITY IDENTIFICATION				
1. Name of Facility				
2. Address of Facility			3. Latitude	
			4. Longitude	
			5. Captain of the Port Zone	
6. Type of Operation (check all that apply)				
<input type="checkbox"/> Break Bulk <input type="checkbox"/> Petroleum <input type="checkbox"/> Certain Dangerous Cargo <input type="checkbox"/> Passengers (Subchapter H) <input type="checkbox"/> If other, explain below:				
<input type="checkbox"/> Dry Bulk <input type="checkbox"/> Chemical <input type="checkbox"/> Barge Fleeting <input type="checkbox"/> Passengers (Ferries)				
<input type="checkbox"/> Container <input type="checkbox"/> LHG/LNG <input type="checkbox"/> Offshore Support <input type="checkbox"/> Passengers (Subchapter K)				
<input type="checkbox"/> RO-RO <input type="checkbox"/> Explosives and other dangerous cargo <input type="checkbox"/> Military Supply				
VULNERABILITY AND SECURITY MEASURES				
7a. Vulnerability			7b. Vulnerability Category	
			<input type="checkbox"/> If other, explain	
8a. Selected Security Measures (MARSEC Level 1)			8b. Security Measures Category	
			<input type="checkbox"/> If other, explain	
9a. Selected Security Measures (MARSEC Level 2)			9b. Security Measures Category	
			<input type="checkbox"/> If other, explain	
10a. Selected Security Measures (MARSEC Level 3)			10b. Security Measures Category	
			<input type="checkbox"/> If other, explain	
VULNERABILITY AND SECURITY MEASURES				
7a. Vulnerability			7b. Vulnerability Category	
			<input type="checkbox"/> If other, explain	
8a. Selected Security Measures (MARSEC Level 1)			8b. Security Measures Category	
			<input type="checkbox"/> If other, explain	
9a. Selected Security Measures (MARSEC Level 2)			9b. Security Measures Category	
			<input type="checkbox"/> If other, explain	
10a. Selected Security Measures (MARSEC Level 3)			10b. Security Measures Category	
			<input type="checkbox"/> If other, explain	

U.S. DEPARTMENT OF HOMELAND SECURITY U.S. COAST GUARD CG-6025A (05/03)	VULNERABILITY AND SECURITY MEASURES ADDENDUM	OMB APPROVAL NO. 1625-0077
<p>An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless it displays a valid OMB control number. The Coast Guard estimates that the average burden for this report is 60 minutes. You may submit any comments concerning the accuracy of this burden estimate or any suggestions for reducing the burden to: Commandant (G-MP), U.S. Coast Guard, 2100 2nd St, SW, Washington D.C. 20593-0001 or Office of Management and Budget, Paperwork Reduction Project (1625-0077), Washington, DC 20503. This form may only be used in addition to form CG-6025, never alone.</p>		
<p>NAME OF FACILITY (Use same Name as Block 1., of CG-6025)</p>		
7a. Vulnerability	7b. Vulnerability Category	
	<input type="checkbox"/> If other, explain	
8a. Selected Security Measures (MARSEC Level 1)	8b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
9a. Selected Security Measures (MARSEC Level 2)	9b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
10a. Selected Security Measures (MARSEC Level 3)	10b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
7a. Vulnerability	7b. Vulnerability Category	
	<input type="checkbox"/> If other, explain	
8a. Selected Security Measures (MARSEC Level 1)	8b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
9a. Selected Security Measures (MARSEC Level 2)	9b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
10a. Selected Security Measures (MARSEC Level 3)	10b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
7a. Vulnerability	7b. Vulnerability Category	
	<input type="checkbox"/> If other, explain	
8a. Selected Security Measures (MARSEC Level 1)	8b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
9a. Selected Security Measures (MARSEC Level 2)	9b. Security Measures Category	
	<input type="checkbox"/> If other, explain	
10a. Selected Security Measures (MARSEC Level 3)	10b. Security Measures Category	
	<input type="checkbox"/> If other, explain	

INSTRUCTIONS FOR THE CG-6025
FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY

This form satisfies the requirements for Facility Vulnerability and Security Measures Summary submission found in the Code of Federal Regulations for Facility Security. Form CG-6025A, Vulnerability and Security Measures Addendum, may be used as a continuation of form CG-6025, in order to submit additional vulnerabilities and security measures. If a facility owner or operator submits a Facility Vulnerability and Security Measures Summary pertaining to more than one facility, form CG-6025, shall be submitted to document each additional facility.

BLOCK 1	Self-Explanatory.	BLOCK 8b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.
BLOCK 2	Street Address.		
BLOCK 3	If available, provide latitude to nearest tenth of a minute.		
BLOCK 4	If available, provide longitude to nearest tenth of a minute.	BLOCK 9a	Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 2 that will mitigate the vulnerability you addressed.
BLOCK 5	Provide the Captain of the Port Zone from the list below in which your facility resides. Their respective zones are described in 33 CFR Part 3.	BLOCK 9b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.
BLOCK 6	Check all applicable operations that are conducted at your facility. If you select other, please explain in the box provided.		
BLOCK 7a	Enter a concise description of a vulnerability identified in your facility's assessment. Provide location information if appropriate.	BLOCK 10a	Enter a concise description of additional selected security measures, if any, that will be applied during MARSEC Level 3 that will mitigate the vulnerability you addressed.
BLOCK 7b	Enter the vulnerability identification code from the KEY to categorically identify the vulnerability you described. More than one category may be used. If you select other, please explain in the box provided.	BLOCK 10b	Enter the security measures identification code from the KEY to categorically identify the security measure you described. More than one category may be used. If you select other, please explain in the box provided.
BLOCK 8a	Enter a concise description of a selected security measure identified in the plan for MARSEC Level 1 that will mitigate the vulnerability you addressed.		

CAPTAIN OF THE PORT ZONE:

Anchorage	Honolulu	Mobile	Puget Sound
Baltimore	Houston-Galveston	Morgan City	San Diego
Boston	Huntington	New Orleans	San Francisco
Buffalo	Jacksonville	New York	San Juan
Charleston	Juneau	Paducah	Sault Ste. Marie
Chicago	Long Island Sound	Philadelphia	Savannah
Cleveland	Los Angeles/Long Beach	Pittsburgh	St. Louis
Corpus Christi	Louisville	Port Arthur	Tampa
Detroit	Memphis	Portland, ME	Toledo
Duluth	Miami	Portland, OR	Valdez
Guam	Milwaukee	Providence	Wilmington
Hampton Roads			

KEY**VULNERABILITY CATEGORY:**

Physical Security	PHS	That part of security concerned with physical measures designed to safeguard personnel; to prevent unauthorized access to equipment, installations, material, and documents; and to safeguard them against terrorism, espionage, sabotage, damage, and theft.
Structural Integrity	STI	The design and material construction characteristics of piers, facilities, and associated structures.
Transportation Infrastructure	TRI	Infrastructure that may be exploited during an attack, other than utilities.
Utilities	UTI	The essential equipment and services that are vital to the operation of the facility.
Radio & Telecommunications	RAT	That part of security concerned with measures to protect radio and telecommunication equipment, including computer systems and networks.
Personnel Protection Systems	PPS	Equipment, Gear, or Systems designed to protect facility personnel (i.e. weapons, body armor).
Procedural Policies	PRP	Plans, Policies, and Procedures for specific operations.
Coordination and Information Sharing	CIS	The ability to coordinate and receive/share information with local/state/federal agencies and other commercial entities.
Preparedness	PRE	Implementation of Plans, Policies, and Procedures through Training, Drills, and Exercises conducted to improve security awareness, prevention, and response.

SECURITY MEASURES

Access Control	ACC	Lighting	LIT
Barriers	BAR	Patrols	PAT
Cargo Control	CAC	Planning, Policies, & Procedures	PPP
Communications	COM	Redundancy	RED
Coordination	COR	Response	RES
Credentiaing	CRE	Stand-off Distance	SOD
Detection	DET	Structural Hardening	STH
Guard Force	GUF	Surveillance	SUR
IT Security	ITS	Training	TRA
Inspections	INS	Vessels/Vehicles	VEV
Intelligence	INT		

[USCG–2003–14732, 68 FR 39322, July 1, 2003, as amended at 68 FR 60543, Oct. 22, 2003]

**PART 106—MARINE SECURITY:
OUTER CONTINENTAL SHELF
(OCS) FACILITIES**

Subpart A—General

Sec.	
106.100	Definitions.
106.105	Applicability.
106.110	Compliance dates.
106.115	Compliance documentation.
106.120	Noncompliance.
106.125	Waivers.
106.130	Equivalents.
106.135	Alternative Security Program.

106.140	Maritime Security (MARSEC) Directive.
106.145	Right to appeal.

**Subpart B—Outer Continental Shelf (OCS)
Facility Security Requirements**

106.200	Owner or operator.
106.205	Company Security Officer (CSO).
106.210	Facility Security Officer (FSO).
106.215	Company or OCS facility personnel with security duties.
106.220	Security training for all other OCS facility personnel.
106.225	Drill and exercise requirements.
106.230	OCS facility recordkeeping requirements.