U.S. DEPARTMENT OF HOMELAND SECURITY U.S. COAST GUARD CG-6025 Rev. (03-09)	**FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY**	OMB APPROVAL NO. 1625-0077 Expires: 01/31/2015

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 (CG-5442), U.S. Coast Guard, 2100 2nd St, SW, Washington, DC 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)*

- ☐ Barge Fleeting
- ☐ Break Bulk (HAZMAT)
- ☐ Break Bulk (non-HAZMAT)
- ☐ Bulk Dry (HAZMAT)
- ☐ Bulk Dry (non-HAZMAT)
- ☐ Bulk Liquid (HAZMAT)
- ☐ Bulk Liquid (non-HAZMAT)
- ☐ Bulk Oil (PETROLEUM) Storage/Transfer
- ☐ Bulk Oil (PETROLEUM) Refinery
- ☐ CDC*-Ammonia, Anhydrous
- ☐ CDC* – Chlorine
- ☐ CDC* – LNG
- ☐ CDC* – LPG
- ☐ CDC* – other LHGs
- ☐ CDC* – Material Poisonous by Inhalation (PIH-TIH)
- ☐ CDC* – Other
- ☐ Chemical Production
- ☐ Container
- ☐ Explosives
- ☐ Military Supply
- ☐ Offshore Support
- ☐ Passengers (Cruise)
- ☐ Passengers (Ferry)
- ☐ Passengers (Other)
- ☐ Radioactive Material – Class 7
- ☐ Ro-Ro
- ☐ If other, explain below:

* Certain Dangerous Cargo

VULNERABILITY AND SECURITY MEASURES

7a. Vulnerability	7b. Vulnerability Category ☐ If other, explain
8a. Selected Security Measures (MARSEC Level 1)	8b. Security Measures Category ☐ If other, explain
9a. Selected Security Measures (MARSEC Level 2)	9b. Security Measures Category ☐ If other, explain
10a. Selected Security Measures (MARSEC Level 3)	10b. Security Measures Category ☐ If other, explain

VULNERABILITY AND SECURITY MEASURES

7a. Vulnerability	7b. Vulnerability Category ☐ If other, explain
8a. Selected Security Measures (MARSEC Level 1)	8b. Security Measures Category ☐ If other, explain
9a. Selected Security Measures (MARSEC Level 2)	9b. Security Measures Category ☐ If other, explain
10a. Selected Security Measures (MARSEC Level 3)	10b. Security Measures Category ☐ If other, explain

Reset

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 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 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 2	Street Address.	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.
BLOCK 3	If available, provide latitude to nearest tenth of a minute.	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 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. For example, a container terminal would most likely need to indicate the following types of operation: CDC - Ammonia, Anhydrous; CDC - Chlorine; CDC - Material Poisonous by Inhalation (PIH-TIH); CDC-Other; Container; Explosives; Radioactive Material - Class 7; and Ro-Ro. If you select other, please explain in the box provided.	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 7a	Enter a concise description of a vulnerability identified in your facility's assessment. Provide location information if appropriate.	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.

CAPTAIN OF THE PORT ZONE:

Baltimore	Honolulu	New Orleans	San Diego
Boston	Houston-Galveston	New York	San Francisco Bay
Buffalo	Jacksonville	North Carolina	San Juan
Cape Fear River	Key West	Northern New England	Sault St. Marie
Charleston	Lake Michigan	Ohio Valley	Savannah
Corpus Christi	Long Island Sound	Pittsburgh	Southeast Alaska
Delaware Bay	Los Angeles-Long Beach	Port Arthur	Southeastern New England
Detroit	Lower Mississippi River	Portland, Oregon	St. Petersburg
Duluth	Miami	Prince William Sound	Upper Mississippi River
Guam	Mobile	Puget Sound	Western Alaska
Hampton Roads	Morgan City		

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
Credentialing	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		