DEPARTMENT OF HOMELAND SECURITY
U.S. Coast Guard

OMB No: 1625-0077
Exp. Date: 11/30/2022

FACILITY VULNERABILITY AND SECURITY MEASURES SUMMARY

FACILITY IDENTIFICATION

1. Name of Facility — Date:

2. Address of Facility

3. Latitude .

4. Longitude .

5. River Name *(if applicable)*

6. River Mile *(if applicable)*

7. Captain of the Port Zone

8. 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 #1

9a. Vulnerability

9b. Vulnerability Category

☐ If other, explain

10a. Selected Security Measures (MARSEC Level 1)

10b. Security Measures Category

☐ If other, explain

11a. Selected Security Measures (MARSEC Level 2)

11b. Security Measures Category

☐ If other, explain

12a. Selected Security Measures (MARSEC Level 3)

12b. Security Measures Category

☐ If other, explain

VULNERABILITY AND SECURITY MEASURES #2 *(if applicable)*

9a. Vulnerability

9b. Vulnerability Category

☐ If other, explain

10a. Selected Security Measures (MARSEC Level 1)

10b. Security Measures Category

☐ If other, explain

11a. Selected Security Measures (MARSEC Level 2)

11b. Security Measures Category

☐ If other, explain

12a. Selected Security Measures (MARSEC Level 3)

12b. Security Measures Category

☐ If other, explain

INSTRUCTIONS FOR 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. Each owner or operator that submits one Facility Security Plan (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 CG-6025 form for each facility covered by the plan (33 CFR § 105.410(f)).

BLOCK 1 Self-Explanatory.

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 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 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 7a Enter a concise description of a vulnerability identified in your facility's assessment. Provide location information if appropriate.

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 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 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 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 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 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 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:

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

KEY

VULNERABILITY CATEGORIES

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 (also known as Cyber security).
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	Other	OTH
Cargo Control	CAC	Patrols	PAT
Communications	COM	Planning, Policies, & Procedures	PPP
Coordination	COR	Redundancy	RED
Credentialing	CRE	Response	RES
Detection	DET	Stand-off Distance	SOD
Guard Force	GUF	Structural Hardening	STH
IT Security	ITS	Surveillance	SUR
Inspections	INS	Training	TRA
Intelligence	INT	Vessels/Vehicles	VEV