

**WESTERN RIVERS  
AREA MARITIME SECURITY PLAN**

**Western Rivers Region  
Eighth Coast Guard District**

**Developed by the  
Western Rivers Area Maritime Security Planning Committee  
(WRAMSPC)**

**Promulgated:**

**TABLE OF CONTENTS**

1000	AREA MARITIME SECURITY .....	1
1100	Purpose.....	1
1200	Western Rivers Area Maritime Security Plan Letter of Promulgation .....	1
1210	Record of Changes.....	2
1300	Authority.....	3
1310	Federal Maritime Security Coordinator (FMSC).....	3
1400	Scope.....	4
1500	Suppositions.....	4
1600	Situation .....	5
1610	Physical Characteristics .....	5
1620	Economic Characteristics.....	7
1630	Ports, Charts and Maps .....	7
2000	AREA MARITIME SECURITY COMMITTEE .....	7
2100	Introduction.....	7
2200	Purpose and Objectives.....	7
2300	Western Rivers Area Maritime Security Committee Charter .....	8
2310	Committee Structure and Procedural Rules.....	9
2320	Relationship to Other Committees.....	9
3000	AWARENESS .....	9
3100	Introduction.....	9
3200	Federal, State & Local Security & Law Enforcement Agency Jurisdiction .....	9
3210	Inland River Vessel Movement Center.....	11
3300	Area Maritime Security (AMS) Assessment .....	11
3310	Maritime Security Assessment Report.....	11
3400	Communications .....	12
3410	Communication of Security Information.....	12
3410.1	Communication With the Public.....	13
3410.2	Communications With Waterway Users.....	13
3410.3	Communications With Commercial Vessels.....	13
3410.4	Communications With Facilities.....	14
3410.5	Communicating with Companies.....	14
3410.6	Role of the Area Maritime Security Committee .....	14
3420	Security Reporting .....	14
3420.1	Procedures for reporting suspicious activity .....	15
3420.2	Procedure for Reporting Breaches in Security.....	16
3430	MARSEC Directives.....	16
3430.1	Procedures for Communicating MARSEC Directives.....	16
3430.2	Procedures for Responding to MARSEC Directives .....	17
3430.3	Role of the Area Maritime Security (AMS) Committees.....	17
3440	MARSEC Levels .....	18
3440.1	Procedures to Communicate Changes in MARSEC Levels.....	19
3440.2	Notification of MARSEC Level Attainment.....	19
3440.3	Role of Area Maritime Security (AMS) Committee .....	20
3500	Sensitive Security Information .....	20
3510	Information Designated as Sensitive Security Information .....	20
3520	Covered Persons.....	23
3520.1	Designation as a Covered Person.....	23

3530	Restrictions on the Disclosure of SSI .....	24
3540	Persons with a “Need to Know” .....	25
3550	Marking SSI .....	25
3560	SSI Disclosed By or To the Coast Guard.....	26
3570	Consequences of Unauthorized Disclosure of SSI .....	27
3580	Destruction of SSI.....	27
3590	Procedures for Communicating SSI Material.....	27
3600	Maritime Security Training for AMS Plan Implementation.....	28
3700	Security Resources.....	28
4000	PREVENTION .....	29
4100	Introduction.....	29
4200	Maritime Security (MARSEC) Level Planning.....	29
4210	Procedures When a Vessel and a Facility are at Different MARSEC Levels .....	29
4220	Requesting Equivalencies and Waivers to MARSEC Directives and Levels.....	29
4300	MARSEC Level 1 .....	30
4310	Roles, Resources, Authorities, and Responsibilities.....	30
4320	Standard Security Procedures for MARSEC Level 1 .....	30
4330	Physical Security Measures .....	31
4340	Operational Security (OPSEC) Measures.....	32
4400	MARSEC Level 2 .....	33
4410	Roles, Resources, Authorities, and Responsibilities.....	33
4420	Standard Security Procedures for MARSEC Level 2 .....	33
4430	Physical Security Measures .....	34
4440	MARSEC 2 Verification and OPSEC Measures .....	34
4500	MARSEC Level 3 .....	35
4510	Roles, Resources, Authorities, and Responsibilities.....	35
4520	Standard Security Procedures for MARSEC Level 3 .....	35
4530	Physical Security Measures .....	36
4540	MARSEC 3 Verification and OPSEC Measures .....	37
4600	Public Access Facility.....	38
4610	Designation of Public Access Facilities.....	38
4620	Vessel Responsibilities When Calling at a PAF .....	39
4630	Compliance and Enforcement.....	40
4640	Vessels Calling at a Non-MTSA Regulated Facility or Location.....	41
4700	Maritime Worker Credentials .....	41
4800	Marine Events .....	42
5000	PREPAREDNESS FOR RESPONSE.....	43
5100	Introduction.....	43
5110	Procedures for Responding to Suspicious Activity .....	43
5120	Procedures for Responding to Breaches of Security.....	43
5200	Transportation Security Incident (TSI).....	44
5210	Procedures for Notification.....	44
5220	Incident Command Activation.....	44
5230	Threats that Do Not Rise to the Level of a TSI .....	45
5300	Most Probable Transportation Security Incident .....	45
5310	Identify Command Structure with Assigned Roles (ICS Flowchart) .....	46

5320	Procedure for Responding to a TSI.....	48
5330	Linkage with Applicable Federal, State, Port & Local Plans .....	48
5400	Maritime Security Exercise Requirements .....	49
5410	Purpose of Exercise Program.....	49
5420	Goals of the AMS Plan Exercise Program.....	50
5430	Exercise Cycle .....	50
5440	Scheduling And Design .....	50
5450	Consideration of Equivalent Response .....	52
5460	Record Keeping .....	52
5470	Linkages Between Family of Plans within the Area.....	52
6000	CRISIS MANAGEMENT AND RECOVERY .....	53
6100	Introduction.....	53
6200	Procedures to Maintain Infrastructure .....	53
6300	Procedures for Recovery of MTS .....	53
7000	COMPLIANCE MEASURES .....	54
7100	Control and Compliance Measures.....	54
7200	Enforcement.....	55
7300	MARSEC Compliance.....	55
8000	PLAN DOCUMENTATION AND MAINTENANCE .....	56
8100	Initial Plan Review and Comment .....	56
8110	Procedures for Continuous Review and Update of the AMS Plan .....	56
8120	Procedures for Continuous Review and Update of the AMS Assessment .....	57
9000	APPENDICES .....	57
9100	WR AMS Executive Steering Committee Members .....	57
9200	Western Rivers Regional Map.....	59
9300	Port Operations and Infrastructure.....	60
9400	Risk-Based Scenarios.....	60
9500	Dangerous Cargos for Security Planning.....	60
9600	FMSC Annexes.....	61
9610	Marine Safety Office Chicago .....	61
9620	Marine Safety Office Huntington .....	61
9630	Marine Safety Office Louisville .....	61
9640	Marine Safety Office Memphis .....	61
9650	Marine Safety Office Mobile .....	61
9660	Marine Safety Office Paducah.....	61
9670	Marine Safety Office Pittsburgh.....	61
9680	Marine Safety Office St. Louis.....	61
9690	Marine Safety Unit Baton Rouge.....	61
9700	Glossary of Terms.....	62
TAB A:	Communicating Security Information (Facilities).....	A-1
TAB B:	Communicating Security Information (Commercial Vessels).....	B-1
TAB C:	Security Reports & Quick Response Card Templates .....	C-1
TAB D:	SSI Non-Disclosure Agreement.....	D-1

TAB E: Consolidated Recommended MARSEC Measures Table.....E-1  
TAB F: Public Access Facility Guidance .....F-1  
TAB G: Recommended FMSC OPSEC Measures (Limited Distribution) ..... G-1

**1000 AREA MARITIME SECURITY****1100 Purpose**

(a) The Western Rivers Area Maritime Security Planning Committee (WRAMSPC) has created this Area Maritime Security (AMS) Plan for the Western Rivers (WR) region of the Eighth Coast Guard District, including portions of the Illinois River within the Ninth Coast Guard District. It is designed to deter, to the maximum extent possible, a Transportation Security Incident (TSI). This Plan will define Federal, State and local governments' obligations, and the contributions and responsibilities of other port stakeholders, to the Maritime Homeland Security (MHS) mission.

(b) A primary purpose of the AMS Plan is to provide a framework for communication and coordination amongst port stakeholders and law enforcement officials, and to identify and reduce vulnerabilities to security threats in and near the Maritime Transportation System (MTS). It is designed to capture the information necessary to coordinate and communicate security procedures at each Maritime Security (MARSEC) Level, complement and encompass facility and vessel security plans within the Western Rivers region and each included Captain of the Port (COTP) zone, and ultimately be integrated into the National Maritime Security Plan. Pursuant to the AMS Plan, MTS stakeholders will take certain actions contingent upon changes in MARSEC Levels and develop unified preparedness strategies to deter and respond to security incidents. Nothing contained in this plan shall be construed as relieving the masters, owners, operators, and agents of vessels, facilities or other port assets from their primary responsibility for the protection and security of such vessels, facilities or assets.

(c) A TSI is defined in the Maritime Transportation Security Act of 2002 (MTSA) as "a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. Examples of a TSI may include:

- (1) An incident affecting a particular mode of transportation or inter-modal structure that significantly disrupts normal operations or may result in closure for a significant time period of a key terminal, waterway, or part of the MTS.
- (2) An actual incident, such as an explosion, MTS blockage, release of a Weapon of Mass Destruction (WMD), hijacking, etc.

(d) Not every threat or incident that violates a security plan, process or perimeter, will necessarily result in a TSI. In creating an AMS Plan, efforts will focus on identifying and implementing measures designed to prevent the occurrence of TSIs. Threats and violations need to be evaluated on a case-by-case basis and responded to accordingly. It is the Federal Maritime Security Coordinator's (FMSC) responsibility to determine if and when an incident occurring in his or her zone is severe enough to warrant designation as a TSI.

**1200 Western Rivers Area Maritime Security Plan Letter of Promulgation**

The letter of promulgation is inserted on the next page.



16700

## Western Rivers Area Maritime Security Plan Letter of Promulgation

Ref: (a) Navigation and Vessel Inspection Circular No. 9-02, Change 1  
(b) Maritime Transportation Security Act, Public Law 107-295  
(c) Title 33 CFR Part 103

1. PURPOSE. This Western Rivers Area Maritime Security (WR AMS) Plan provides guidance for the communication and coordination of scalable actions to detect, deter, prevent and respond to threats at varying threat levels for ports within the Western Rivers Area of Responsibility (AOR).
2. ACTION. Each Captain of the Port in their officially designated role as the Federal Maritime Security Coordinator (FMSC) within the Western Rivers shall adopt the maritime security concepts and mitigating strategies described in this plan, and shall promote compliance.
3. DIRECTIVES AFFECTED. None.
4. BACKGROUND. The terrorist attacks of September 11, 2001 compelled the Coast Guard to re-evaluate and strengthen the ability for protection of our nation's ports, waterways and coastal areas from possible attack. In December 2001, the Commandant reaffirmed the Coast Guard's Maritime Homeland Security mission. The mission is to work in coordination with the Department of Defense (DOD), federal, state and local agencies, owners and operators in maritime industry, and others with interests in our nation's marine transportation system to detect, deter, prevent and respond to attacks against U.S. territory, population and critical maritime infrastructure by terrorist organizations. To accomplish this mission and associated goals, the Commandant directed that AMS Plans be developed and exercised by AMS Committees.
5. DISCUSSION. The contents of this WR AMS Plan apply to all ports within the Western Rivers. Each Captain of the Port within the Western Rivers is authorized to amplify these provisions within their individual AOR.
6. CHANGES. Changes may be proposed in writing and submitted to the WR AMS Committee Chair.
7. FORMS AND REPORTS. None.

F. M. PASKEWICH  
Captain, U.S. Coast Guard  
Inland Waterways Coordinator



### 1300 Authority

Section 102 of the Maritime Transportation Security Act of 2002 (MTSA), P.L. 107-295, codified at 46 USC §§ 70101 –70117, mandates the development of a National Maritime Transportation Security Plan, Area Maritime Security Plans, and Facility and Vessel Security Plans. The Coast Guard is designated as the Lead Federal Agency (LFA) responsible for implementation of the MTSA. The COTPs, acting as Federal Maritime Security Coordinators (FMSC), are responsible for developing AMS Plans with advice from AMS Committees. The AMS Plan will be consistent with the National Maritime Transportation Security Plan and the National Transportation Security Plan. The Eighth and Ninth Coast Guard Districts have elected to combine all or portions of nine FMSC zones within the Western Rivers to develop a regional AMS Plan.

### 1310 Federal Maritime Security Coordinator (FMSC)

(a) Each COTP under this plan (listed below with contact numbers) is designated as the FMSC in their zone. Any FMSC Zone or FMSC area referred to in this plan corresponds to the COTP Zone defined in Title 33 Code of Federal Regulations (CFR) Subpart 3.40. In addition to other authorities prescribed for the COTP, the FMSC is authorized to:

- (1) Establish, convene and direct a local AMS Committee (considered a sub-committee of the WR AMS Committee)
- (2) Appoint members to the AMS Committee
- (3) Develop and maintain an FMSC-specific annex to the WR AMS Plan.
- (4) Implement and exercise the specific annex to the WR AMS Plan.
- (5) Maintain the records required under 33 CFR Part 103.520

(b) These security responsibilities are in addition to key responsibilities for traditional Coast Guard missions and are fundamental to the success of the maritime homeland security program. To accomplish the goals outlined in the Coast Guard's Maritime Strategy for Homeland Security, the FMSC must rely on fellow Federal, State and local representatives, and other maritime area partners to assist whenever possible.

Unit	Business Hours	24-Hour (Operational/Urgent Calls)
MSO Chicago	(630) 986-2155	(630) 986-2155
MSO Huntington	(304) 529-5524	Group Ohio Valley: (502) 582-6439 ext. 222
MSO Louisville	(502) 582-5194	(502) 376-9793
MSO Memphis	(901) 544-0555	(901) 544-3912 ext 2124
MSO Mobile	(251) 441-5770	(251) 441-5121
MSO Paducah	(270) 442-1621	(270) 994-7385
MSO Pittsburgh	(412) 644-5808	Group Ohio Valley: (502) 582-6439 ext. 222
MSO St. Louis	(314) 539-3091 ext. 1	Group Upper Mississippi: (319) 524-7511 ext. 6
MSU Baton Rouge (a sub-unit of MSO New Orleans)	(225) 298-5400  (504) 589-4256	(504) 589-6261  (504) 589-6261

**1400 Scope**

- (a) The AMS Plan by its nature is very broad in scope, encompassing the whole of the maritime domain within the Western Rivers region, and absorbing the individual assessments and planning efforts of facilities and vessels operating within that area. The scope of each FMSC Annex to the plan is determined by evaluating the waterways, facilities, vessels, and adjacent areas that may be involved in, or affected by, a TSI in the FMSC zone.
- (b) The plans required by 33 CFR Parts 104 and 105 provide the foundation of the overarching AMS Plan. However, the AMS Plan must extend beyond the required facility and vessel security plans, and develop strategies to reduce the vulnerabilities of the weakest elements of the port, including those vessels, facilities and infrastructure that are not regulated under 33 CFR Parts 104 and 105.

**1500 Suppositions**

- (a) The following suppositions provide the foundation for the Coast Guard's approach to its MHS mission and successful implementation of the MTSA:
- (1) Ports are very open and may be susceptible to a TSI, which may occur at any time with little or no warning.
  - (2) Protection of human life and health are the most important considerations in AMS Plan development and execution.
  - (3) Maintaining continuity of operations and facilitating commerce in the port area is a critical consideration.
  - (4) Security must be maintained during response and crisis management incidents.
  - (5) It is in the best interest of the United States to increase port security by establishing and improving communications among law enforcement officials responsible for port security.
  - (6) Each entity (or representative thereof, such as trade/professional organizations) directly or indirectly involved with the MTS will participate with the AMS Committee to increase awareness and enhance prevention of illegal acts.
  - (7) The National Oil and Hazardous Material Contingency Plan (NCP), Federal Response Plan / National Response Plan (FRP/NRP), Interagency Domestic Terrorism Concept of Operations Plan (CONPLAN) and other response plans will be activated for the purpose of response and crisis management due to a TSI.
  - (8) Many private and government entities at the local, state and federal level share the authority, resources and expertise to effectively combat terrorism, and will respond jointly to incidents.
  - (9) All port areas are susceptible to air attack.
  - (10) There will be a competition for security resources as threat levels increase.
  - (11) There are a variety of characteristics of the Western Rivers system that influence MARSEC attainment strategies. The rivers are a "closed, linear system", generally bounded by banks within sight of each other, access is limited to established

entrance and exit points, and transit is directionally limited to upbound and downbound axes. Surveillance sites are easily and quickly approached by land along the entire system. Vessels of special interest can be readily observed without detection, and, if warranted, surveillance areas could be used as steady aim sites or boat and helo launching sites for special interventions.

(12) Marine traffic in the Rivers system has been subjected to "layered defense" mechanisms before entering the system. Approaching marine traffic will have already been vetted thru various means to sort out the benign from those in which we have greater interest. All commercial traffic in the system is under the control of US citizens and is subject to routine and frequent CG oversight. As in the coastal environment, foreign shipping approaching and transiting the early part of the Rivers system is under the control of US pilots and susceptible to all boarding and control mechanisms employed by CG Forces.

(13) There are well-known and well-defined control points, determined by natural and geographic features which limit speed and freedom of motion for all vessels along the route; tight bends, bottom formations, current to be negotiated, channel restrictions, etc. The system contains hundreds of isolation mechanisms; pooled waters, locks & dams, and density of marine traffic which all provide built-in, automatic restriction mechanisms that permit instant isolation of high interest vessels. Ordinary transit requires positive assistance by Government agents (ACOE lock operators) to allow continued transit.

## **1600 Situation**

The complexity, scope, and potential consequences of a terrorist threat or TSI occurring within the Maritime Transportation System (MTS) requires that there be a coordinated effort between all MTS users and law enforcement agencies. This effort will require open communication, enhanced awareness of potential threats and coordinated procedures for prevention, preparedness, response and recovery. It will require those involved to fully understand their roles in enhancing security. An essential tool for achieving optimum coordination are the MARSEC Levels developed by the Coast Guard, more fully discussed in section 3440.

### **1610 Physical Characteristics**

(a) The WR region includes all or portions of nine FMSC zones. Each of these FMSC zones includes all facilities and MTS infrastructures adjacent to navigable waterways in their associated AOR. Section 2300 (Western Rivers Area Maritime Security Committee Charter) includes a description of the FMSC zones covered by this plan. Each FMSC Annex contains additional information on their respective areas. Ports within the WR share many inherent commonalities. These MTS infrastructures, vessels, cargo and facility interfaces, along with associated waterfront areas are:

- (1) U.S. Military Facilities
- (2) Passenger Vessels – Subchapter T, H, K
- (3) Permanently Moored Vessels (PMV)
- (4) Towing Vessels
- (5) Recreation Vessels

- (6) High-density population areas
  - i) City populations greater than 100,000
  - ii) Visitor populations due to seasonal attractions or special events
- (7) Special event locations
- (8) Nuclear Power Plants
- (9) Marine Transfer Related (MTR) Facilities
  - i) Oil Transfer & Storage
  - ii) Chemical Transfer & Storage
  - iii) Oil Production
  - iv) Chemical Production
- (10) Marine Terminals
- (11) Locks/Dams/Dikes/Levees/Waterway Infrastructure
- (12) Power Generation
- (13) Power Distribution
- (14) Fleeting Areas
- (15) Non-regulated Waterfront Facilities
- (16) Grain/Aggregate Facilities
- (17) Shipyards/Rail Yards/Tank Cleaning and Stripping Facilities
- (18) Bridges
  - i) Major – Eisenhower Defense Transportation System and prioritized railroad bridges
  - ii) Minor – other than those categorized as “major”
- (19) Channels/Canals/Inland Waterways System/Chokepoints/Aids to Navigation
- (20) Petroleum Transportation Infrastructure – pipelines
- (21) Public/Private Utilities and related infrastructure
- (22) Barges
  - i) Certain Dangerous Cargo (CDC) barge
  - ii) Tank barge (“Red Flag”)
  - iii) Hopper barge

(b) In addition to certain requirements for CDC tows to communicate with IRVMC, all Masters or Pilots of commercial vessels must check-in with individual lockmasters for passage. Communications are available at all operational locks through VHF-FM radio 156.8 MHz (Ch. 16) and 156.65 MHz (Ch. 13). Masters of vessels shall furnish to the lockmaster such statistics of passengers or cargo as may be requested. Any commercial or recreational vessel desiring lockage may make radio contact. Commercial tows are required to make contact at least one half hour before arrival at a lock in order that the master may be informed of current river and traffic conditions that may affect the safe passage of his tow. No means are currently available to track recreational traffic.

(c) Refer to individual FMSC annexes for a detailed description of port physical characteristics, including areas of responsibility for each local AMS Committee.

(d) Descriptions of the FMSC zones incorporated in this plan are included in Section 2300 (WR AMS Committee Charter).

**1620 Economic Characteristics**

The WR MTS is an integral part of the economic vitality of the United States. FMSC zones within the WR share many inherent commonalities unique from those of coastal ports. Refer to section 1610 for a list of economic and MTS infrastructure commonalities. In addition, each individual sub-port may possess unique port activities or MTS infrastructure that will be addressed in the individual FMSC annex.

**1630 Ports, Charts and Maps**

Refer to Appendix 9200 for charts of the WR region. Refer to applicable annexes for specific FMSC zone charts or maps.

**2000 AREA MARITIME SECURITY COMMITTEE****2100 Introduction**

AMS Committees are essential tools for the development and execution of AMS Plans, and for achieving an enhanced level of security within the maritime domain. As such, the Commander, Eighth Coast Guard District has established the Western Rivers Area Maritime Security (WR AMS) Committee to advise the Coast Guard on regional maritime security matters. Each FMSC under this plan shall establish local AMS Committee(s) to address issues particular to their area of responsibility. These will be considered as sub-committees of the WR AMS Committee.

**2200 Purpose and Objectives**

- (a) The AMS Committee brings together appropriately experienced representatives from a variety of sources in the region to continually assess security risks to the ports, determine appropriate risk mitigation strategies, and develop, revise, and implement the AMS Plan. The AMS Committee also serves as a mechanism by which security threats and changes in MARSEC Levels are communicated to port stakeholders.
- (b) The objectives of the AMS Committee include:
  - (1) Assisting in the development, review, and update of the AMS Plan, aimed at maintaining acceptable risk levels during normal operations and during times of heightened threats. The AMS Plan will outline scalable security procedures to be taken by regulated entities at each MARSEC Level. The procedures will meet consolidated requirements of all agencies having jurisdiction.
  - (2) Assisting with a comprehensive AMS Assessment. These assessments must detail the threats, vulnerabilities, and consequences associated with each port area within a FMSC zone. This requirement may be met using the Risk-Based Decision-Making methodologies developed by the Coast Guard or other appropriate Risk Based Decision Making Tools.
  - (3) Integrating and/or amending existing security assessments of maritime facilities using agreed upon criteria.
  - (4) Developing information sharing procedures for threat warnings, response, intelligence gathering, and threat assessment among public and private entities.

- (5) Soliciting stakeholder recommendations for continuing improvements of AMS measures.
- (6) Promoting effective security measures that maintain or enhance operational efficiencies and minimize impact to legitimate trade.
- (7) Advising, consulting with, and reporting to the Coast Guard Eighth District Commander and FMSCs on matters relating to maritime security.
- (8) Assisting the District Commander and FMSCs with the communication of security information to the port and waterway stakeholders.

**2300 Western Rivers Area Maritime Security Committee Charter**

The WR AMS Committee Charter is inserted beginning on the next page.

## **Western Rivers Area Maritime Security Committee Charter**

The Western Rivers Area Maritime Security (AMS) Committee, hereinafter referred to as the “AMS Committee,” is hereby chartered, effective January 30, 2004, in accordance with 33 CFR 103.300(b). The AMS Committee provides a forum for port stakeholders in the Western Rivers Region to work together in facilitating the Coast Guard’s Ports, Waterways, and Coastal Security (PWCS) mission to deter, detect, prevent and respond to attacks against U.S. territory, population, and critical maritime infrastructure.

### **A. References:**

Ref: (a) 33 CFR Part 103, Area Maritime Security  
(b) Navigation and Vessel Inspection Circular (NVIC) 9-02 Change 1, Guidelines for Development of Area Maritime Security AMS Committees, and Area Maritime Security Plans Required for U.S. Ports

### **B. Responsibilities:**

1. The AMS Committee will:

- a. Function as the regional AMS Committee for the Western Rivers Region. As such, it will incorporate the geographic boundaries of the Captain of the Port (COTP) zones of Pittsburgh, Huntington, Paducah, Louisville, St. Louis, and Memphis, as described below. In addition, certain rivers portions of the COTP zones of Chicago, Mobile, and New Orleans will be incorporated into the Committee. The AMS Committee will be comprised of an “Executive Steering Committee” of voting members, and “At-Large” non-voting members. The Committee will serve as an oversight body for the Area Maritime Security Subcommittees within the region that operate under the COTPs. The COTPs will remain the Federal Maritime Security Coordinators (FMSC) for their respective COTP zones described in 33 CFR Part 3, including all ports and areas located therein, and will oversee all AMS Subcommittee activities.
- b. Coordinate maritime security activities among Western Rivers COTP zones to assure consistency in:
  - (1) Identifying critical port infrastructure and operations.
  - (2) Identifying risks (threats, vulnerabilities, and consequences).
  - (3) Determining mitigation strategies and implementation methods.
  - (4) Developing and describing the process to continually evaluate overall port security
- c. Prepare and maintain a Western Rivers Area Maritime Security Plan, hereinafter referred to as the “AMS Plan,” incorporating annexes developed by the COTPs. The AMS Plan will address port security issues and security operating procedures common to all COTP offices in the region.
- d. Provide a regional focus to the COTPs in their efforts to complete risk-based AMS Assessments.
- e. Provide advice to individual AMS Subcommittees throughout the region so they can assist the COTPs in developing, reviewing, and updating their individual annexes to the AMS Plan.
- f. Foster a system-wide approach to maritime security within the region that emphasizes regional strategies and resources.
- g. Serve as a link in communicating threats and changes in Maritime Security (MARSEC) levels, and disseminating appropriate security information to the AMS Subcommittees through the COTPs.

### **C. Objectives:**

1. The objectives of the AMS Committee are to:

- a. Assist in the development, review, and update of the AMS Plan aimed at maintaining acceptable risk levels during normal operations and during times of heightened threats. The AMS Plan will outline scalable security procedures to be taken by Marine Transportation System (MTS) stakeholders to ensure the continued safety and security of the region's port areas and the MTS.
- b. Assist with a comprehensive Western Rivers AMS Assessment. This assessment must detail the threats, vulnerabilities, and consequences associated with the region. This requirement may be completed using the risk based decision-making methodologies developed by the Coast Guard.
- c. Integrate and/or amend existing security assessments of maritime facilities using agreed criteria.
- d. Develop and adopt preventative security measures for appropriate MARSEC Levels to address increased threat conditions. The measures will meet consolidated requirements of all agencies having jurisdiction.
- e. Develop information sharing procedures for threat warnings, response, intelligence gathering, and threat assessment among public and private entities.
- f. Solicit stakeholder recommendations for continuing improvement of AMS measures.
- g. Promote effective security measures that maintain or enhance operational efficiencies and minimize impact to legitimate trade.
- h. Advise, consult with and report to the District Commander on matters relating to maritime security in the region.
- i. Assist the District Commander with the communication of security information to the ports and waterway stakeholders.
- j. Ensure consistent application of the MTSA regulations throughout the Western Rivers Region.

**D. Geographic Areas of Responsibility:**

1. The Western Rivers Region includes the following COTP zones and associated areas of responsibility. Each of these COTP zones includes all facilities and MTS infrastructure adjacent to those waterfronts.

a. COTP Huntington Zone – includes all waters, tributaries and adjacent waterfront from mile markers 121.6 to 374.8 of the Ohio River; mile markers 00.0 to 90.5 of the Kanawha River; mile markers 00.0 to 10.0 of the Big Sandy River; mile markers 00.0 to 3.0 of the Elk River; mile markers 00.0 to 2.0 of the Muskingum River; and mile markers 00.0 to 4.0 of the Little Kanawha River.

b. COTP Louisville Zone – includes all waters, tributaries and adjacent waterfront from mile markers 374.8 to 867.3 of the Ohio River; mile markers 00.0 to 258.6 of the Kentucky River; mile markers 00.0 to 3.0 of the Licking River; mile markers 00.0 to 117.6 of the Miami River; mile markers 00.0 to 585.0 of the Wabash River; mile markers 00.0 to 51.6 of the White River; mile markers 00.0 to 29.0 of the Rough River; and mile markers 00.0 to 100.0 of the Green River. Navigable lakes include Lake Cumberland and Lake Dale Hollow. COTP Louisville zone contains the following sub-zone which is assigned specific oversight for the AOR as indicated:

(1) MSD Cincinnati, OH - mile markers 374.8 to 531.5 of the Ohio River.

c. COTP Memphis Zone – includes all waters, tributaries and adjacent waterfront from mile markers 507.0 to 882.7 of the Lower Mississippi River; the north Memphis area of the Wolf River; the McClellan-Kerr Navigation System of the Arkansas River; the east Arkansas portion of the White River; the southwest Arkansas section of the Red River; the south central Arkansas area of the Ouachita River; and the south central Mississippi (state) portion of the Yazoo River north of Laflore County. COTP Memphis Zone contains the following sub-zones which are assigned specific oversight for the AOR as indicated:

(1) MSD Greenville, MS – mile markers 507.0 to 661.8 of the Lower Mississippi River; mile markers 00.0 to 57.0 of the White River; and mile markers 00.0 to 51.0 of the Arkansas River.

(2) MST Fort Smith, AR - mile markers 113.0 to Oklahoma City, OK, and the McClellan-Kerr Navigation System on the Arkansas River to the Vertigres River.

d. COTP Paducah Zone – includes all waters, tributaries and adjacent waterfront from mile markers 882.7 to 953.8 of the Lower Mississippi River; mile markers 00.00 to 55.3 of the Upper Mississippi River; mile markers 867.3 to 981.0 of the Ohio River; mile markers 00.00 to 80.0 of the Tennessee River; and mile markers 00.0 to 80.0 of the Cumberland River. COTP Paducah zone contains the following sub-zone which is assigned specific oversight for the AOR as indicated:

(1) MSD Nashville, TN - mile markers 80.0 to 385.7 of the Cumberland River; mile markers 80.0 to 652.2 of the Tennessee River; and mile markers 412.0 to 450.5 of the Tennessee-Tombigbee Waterway.

e. COTP Pittsburgh Zone – includes all waters, tributaries and adjacent waterfront from mile markers 00.0 to 121.6 of the Ohio River; mile markers 00.0 to 128.7 of the Monongahela River; and mile markers 00.0 to 72.0 of the Allegheny River.

f. COTP St. Louis Zone - includes all waters, tributaries and adjacent waterfront from mile markers 55.3 to 343.0 of the Upper Mississippi River; mile markers 00.0 to 489.8 of the Missouri River; and mile markers 00.0 to 65.0 of the Illinois River. Navigable lakes include Lake of the Ozarks, Table Rock Lake, Bull Shoals Lake, Norfolk Lake and Lake Tanicomo in Missouri. COTP St. Louis Zone contains the following sub-zones which are assigned oversight for the AOR as indicated:

(1) MSD Peoria, IL – mile markers 65.0 to 187.0 of the Illinois River.

(2) MSD Quad Cities, IL – mile markers 343.0 to 615.0 of the Upper Mississippi River; and mile markers 489.8 to 734.0 of the Missouri River.

(3) MSD St. Paul, MN – mile markers 615.0 to 857.6 of the Upper Mississippi River; and mile markers 734.0 to 980.0 of the Missouri River.

g. The rivers portions of the following COTP zones will be incorporated into the WRAMS Plan:

COTP Chicago – The portion of the Des Plains River from the Brandon Road Locks and Dam at mile marker 286, south to mile marker 187.2 of the Illinois River.

COTP Mobile – All rivers north of the mouth of the Mobile River.

COTP New Orleans – all rivers north of the 190 bridge on the Mississippi River in Baton Rouge, Louisiana.

#### **E. Rules of Membership:**

1. Rules of Membership are subject to all relevant sections of 46 USCA §§ 70101 et. seq and 33 CFR Subchapter H.

2. The AMS Committee is exempt from the Federal Advisory Committee Act (FACA), Public Law 92-436, 86 Stat.470 (5 U.S.C. App.2) but is subject to the formal rules mandated under 33 CFR 103.

3. The AMS Committee shall at all times consist of at least seven members who have 5 years of experience related to maritime or port security operations. Additional members need not meet the experience requirement.

4. While membership on the AMS Committee is currently limited to representatives of the agencies and organization listed below, membership on COTP AMS Subcommittees is open to any interested commercial entity, government agency, or other marine transportation system stakeholder operating on, or along, or having jurisdiction within the AMS Committee's Area of Responsibility (AOR).

5. Membership of the AMS Committee will be comprised of:

**Executive Steering Committee:** <sup>(1)</sup>

Eighth Coast Guard District Inland Waterways Coordinator <sup>(2)</sup>  
Transportation Security Administration  
Maritime Administration  
U.S. Army Corps of Engineers Mississippi Valley Division  
U.S. Army Corps of Engineers Great Lakes and Ohio River Division  
Northern Command  
Transportation Command  
Bureau of Customs and Border Protection  
Towing Safety Advisory Committee  
Chemical Transportation Advisory Committee  
American Waterways Operators  
Passenger Vessel Association  
American Gaming Association  
Inland Rivers Ports and Terminals  
Barge Fleeting Representative

**At-Large Committee:**

COTP Pittsburgh <sup>(2)</sup>  
COTP Huntington <sup>(2)</sup>  
COTP Louisville <sup>(2)</sup>  
COTP Paducah <sup>(2)</sup>  
COTP St. Louis <sup>(2)</sup>  
COTP Memphis <sup>(2)</sup>  
COTP Chicago <sup>(3)</sup>  
COTP Mobile <sup>(3)</sup>  
COTP New Orleans <sup>(3)</sup>  
USCG Group Ohio Valley  
USCG Group Lower Mississippi River  
USCG Group Upper Mississippi River  
USCG Auxiliary  
Commandant (G-MP)  
Atlantic Area (Am)  
Department of Homeland Security  
Environmental Protection Agency  
Office of Pipeline Safety  
Research and Special Projects Administration  
American Chemical Council  
Federal Railroad Administration  
Federal Highway Administration  
Federal Emergency Management Agency  
Federal Bureau of Investigation  
Nuclear Regulatory Commission  
Tennessee Valley Authority

<sup>(1)</sup> Executive Steering Committee members will have voting authority to conduct committee business; At-Large Committee members will not.

<sup>(2)</sup> Indicates a position-specific assignment. All other agencies and organizations will designate a single representative to serve on the AMS Committee.

<sup>(3)</sup> The rivers portions of the areas of responsibility for COTP Chicago, COTP Mobile, and COTP New Orleans will be incorporated into the WRAMS Plan. Representatives from those units will serve as “At-Large” committee members.

6. Members’ terms of office will be for 5 years; however, to permit orderly turnover of the AMS Committee’s membership, the initial terms of office will be staggered, and the members initially appointed to the AMS Committee will be appointed to terms of 3, 4 or 5 years. Members will be eligible to serve an additional term of office.
7. Members shall be formally appointed in writing by the Eighth Coast Guard District. In making appointments, the District shall consider the skills required by 33 CFR 103.410.
8. Members will not receive any salary or other compensation for their services on the AMS Committee.
9. Meetings will be held once a quarter for the first year beginning February 2004, and then a minimum of once a year thereafter, or on an “as needed” basis as determined by the membership.
10. The Chairperson position will be permanently filled by the Eighth District Inland Waterways Coordinator.
11. The Vice Chairperson position will be filled by one of the members of the Executive Steering Committee and will rotate every two years.
12. The Executive Secretary position will be permanently filled by the Eighth District Port Security Specialist having responsibility for the inland rivers.

**F. Area Maritime Security Subcommittees:**

1. Each COTP in the Western Rivers Region will maintain one or more AMS Subcommittees in his or her COTP zone. While reporting to the COTPs, AMS Subcommittees will also serve as subcommittees of the AMS Committee.
2. AMS Subcommittee members will be appointed by the COTP on a volunteer basis. Appointment will be highly informal and based on the members’ willingness to serve.
3. AMS Subcommittee members are not subject to the formal Rules of Membership in Paragraph E, above. The COTPs will establish their own rules for membership on the AMS Subcommittees.
4. Any member of the AMS Committee is also eligible for membership on any AMS Subcommittee.
5. AMS Subcommittees may designate subcommittees to address specialized functional areas such as intelligence and law enforcement, facilities and infrastructure, vessel operations, etc.
6. The responsibilities of AMS Subcommittees include but are not limited to:
  - a. Develop an Area Maritime Security Assessment in accordance with 33 CFR Part 103, subpart D, or review and/or comment upon any existing assessment.
  - b. Identify critical maritime area infrastructure and operations, and identify risks (threats, vulnerabilities, and consequences) in the maritime sector.
  - c. Advise the FMSC on mitigation strategies appropriate to these risks and implementation methods.
  - d. Develop and describe the process for continual evaluation and update of overall port security vulnerabilities and mitigations, how they change over time, and what additional security enhancing strategies can be applied.
  - e. Provide advice to and assist the FMSC in developing annexes to the AMS Plan in accordance with 33 CFR Part 103, Subpart E.
  - f. Serve as the principle link for communicating threats and changes in MARSEC levels, and disseminating appropriate security information to maritime stakeholders.

- g. Design and recommend to the FMSC measures to assure effective security of infrastructure, special events, vessels, passengers, cargo and cargo handling equipment at facilities within the port and not otherwise covered under federally approved Vessel or Facility Security Plans.
- h. Serve as the principle link for communicating the approved AMS Plan, including any requirements for entities operating in the maritime area contained in the AMS Plan.
- i. Assist maritime entities operating in the area with understanding and complying with federal, state, and local security regulations and requirements.
- j. Coordinate and conduct an AMS Exercise at least once each calendar year.
- k. Maintain records of AMS Subcommittee operations and decisions.
- l. Ensure that all sensitive information is afforded the appropriate level of protection.
- m. Submit a report to the AMS Committee annually by 31 December to highlight subcommittee activities for the previous calendar year.

**G. Responsibilities of Committee Positions:**

1. Chairperson. The Chairperson will have oversight of AMS Committee. He or she is responsible for:
  - a. Establishing, convening, and directing the AMS Committee.
  - b. Appointing members to the AMS Committee.
  - c. Developing and maintaining, in coordination with the AMS Committee, the AMS Plan.
  - d. Implementing and exercising the AMS Plan.
  - e. Maintaining the records required by 33 CFR 103.520.
2. Vice Chairperson. The Vice Chairperson shall act as Chairperson in the absence or incapacity of the Chairperson, or in the event of a vacancy in the office of the Chairperson.
3. Executive Secretary. The Executive Secretary shall be responsible for the administrative duties of the AMS Committee. The duties of the Executive Secretary include the following:
  - a. Maintain current AMS Committee designation letters.
  - b. Publish meeting locations, times, and dates.
  - c. Conduct roll call and maintain visitor attendance logs.
  - d. Assist the Chairperson and Assistant Chairperson in conducting meeting business.
  - e. Ensure the minutes are documented, which need not be verbatim, but shall reflect the essence of the discussion and any recommendations or decisions made with respect to each subject considered.
  - f. Ensure meeting minutes are distributed to members prior to each meeting.
  - g. Communicate port security information to the AMS Committee members as directed by the Chairperson and Vice Chairperson.
  - h. Maintain the current edition of AMS Plan.
  - i. Assure that all AMS Committee records are maintained as SSI where appropriate.
4. AMS Committee Members. AMS Committee members will at all times adhere to the requirements of reference (a), and the guidance provided in reference (b).
  - a. AMS Committee members are responsible for planning and coordinating security procedures and are not considered a response entity for purposes of crisis management.

**H. Order of Business:**

1. The order of business at regular meetings of the AMS Committee will be:
  - a. Self-introduction of attendees

- b. Acceptance of the agenda
- c. Reading/Acceptance of minutes
- d. Subcommittee and Task Force reports
- e. Old business
- f. New business
- g. Adjournment

**I. Meetings:**

1. Meetings may be open to the public; however, discussions of SSI materials will limit attendees to those with a need to know who have an approved SSI form on file.
2. The attendance of a simple majority of the AMS Executive Steering Committee shall constitute a quorum for the transaction of business at any scheduled meeting. If less than a simple majority of the Executive Steering Committee members are in attendance at any scheduled meeting a simple majority of the members in attendance may adjourn the meeting to another time.
3. The act or business of a simple majority of the Executive Steering Committee members present at a scheduled meeting will be the act of the entire Executive Steering Committee membership.
4. Ad hoc meetings of the partial AMS Executive Steering Committee may be called at any time to address Committee business; however, a simple majority of members in attendance does not, in that instance, constitute a quorum for conducting AMS Executive Steering Committee business. Business conducted at ad hoc meetings of the partial Executive Steering Committee must be voted on by a quorum of the full AMS Executive Steering Committee at a regularly scheduled meeting.

**J. Guidelines for Public Access to AMS Committee Meetings and Records:**

1. AMS Committee and AMS Subcommittee meetings may be open to the public, and records of meetings may be made available to the public upon request. However, the AMS Committee shall ensure that all material designated as SSI, and all references to SSI material are redacted from records prior to disclosure to the public.
2. Only individuals who have been determined by the AMS Committee as covered persons with a need to know will be allowed access to SSI, including any material or AMS Committee records that pertain to SSI.

**K. Procedural Rules of Order:**

1. General meetings of the AMS Committee are conducted by utilizing Robert's Rules of Order. The following is a list of procedures to be followed
  - a. Policy. It is the policy of the AMS Committee that general members of the public shall have the opportunity to speak to any general membership meeting agenda item before final action.
  - b. Spokesperson for a Group of Persons. When any group of persons wishes to address the AMS Committee on the same subject matter, it shall be proper for the presiding officer to request that a spokesperson be chosen by the group to address the AMS Committee.
  - c. Scheduling of Closed Session. Special closed sessions shall be scheduled as necessary in conjunction with general membership meetings.
  - d. Matters not on the Agenda. No substantive matters other than those on the agenda shall be finally acted upon by the AMS Executive Steering Committee; provided, however, that matters deemed to be of an urgent nature or emergencies by any appointed member of the AMS Committee, with an explanation of the emergency or urgency stated in the meeting, be considered and acted upon by the AMS Committee.
  - e. Presiding Officer (Chair) to State Motion or Issue. The Presiding Officer shall assure that all motions or issues are clearly stated before allowing debate and discussion to begin. The Presiding Officer may restate the motion or issue, or may direct that an AMS Committee member restate the motion before allowing discussion to

continue. The Presiding Officer shall restate the motion prior to voting.

f. Presiding Officer (Chair) May Discuss and Vote. The Presiding Officer may move, second and discuss from the chair, subject only to such limitations of debate as are by these rules imposed on all members. The Presiding Officer shall not be deprived of any of the rights and privileges of a member.

g. Manner of Voting. On the passage of every incidental motion or recommendation, the vote or recommendation shall be taken by voice and entered in full upon the record. On the passage of substantive issues requiring input by the AMS Subcommittees, the AMS Subcommittee Chair shall provide the AMS Committee with the vote or recommendation.

h. Silence Constitutes Affirmative Vote. Appointed members of the AMS Executive Steering Committee who are silent during a voice vote shall have their vote recorded as an affirmative vote, except when individual appointed members have stated in advance that they will not be voting.

i. Failure to Vote. It is the responsibility of every appointed member of the AMS Executive Steering Committee to vote unless disqualified for cause accepted by the Executive Steering Committee by opinion of a cognizant attorney. No appointed member can be compelled to vote.

j. Abstaining from Vote. The abstainer chooses not to vote and, in effect, "consents" that a majority of the quorum of the appointed members present may act for him or her.

k. Not Participating. An appointed member who disqualifies himself or herself because of any financial or other interest in the issue at hand shall disclose the nature of the conflict and may not participate in the discussion or the vote. An appointed member may otherwise disqualify him or herself due to personal bias or the appearance of impropriety.

l. Tie Votes. Members of the AMS Executive Steering Committee may reconsider tie votes. If the tie vote resulted from a general "aye" or "nay" vote, a motion may be made to reconsider the vote with individual votes being counted orally. A member may also motion to continue the matter to another date. Nothing herein shall be construed to prevent any appointed member from adding a matter to the agenda that resulted in a tie vote for a subsequent meeting.

m. Motion to Reconsider. A motion to reconsider any action taken by the AMS Committee may be made only during the meeting when the action was taken. A motion to reconsider requires a second, is debatable and is not amendable. Such motion must be made by one of the prevailing side, but may be seconded by any appointed member. A motion to reconsider may be made at any time and shall have precedence over all other motions, or while a member has the floor, providing that no vested rights are impaired. The purpose of reconsideration is to bring back the matter for review. If a motion to reconsider fails, it may not itself be reconsidered. Reconsideration may not be moved more than once on the same motion. Nothing herein shall be construed to prevent any appointed member from making a motion to rescind such action at a subsequent meeting of the council.

#### **L. Rules for Handling and Protecting Classified, Sensitive Security, Commercially Sensitive, and Proprietary Information:**

1. Authorized Closed Sessions. Subject to the advice of the Chairman and the requirements of 49 CFR 1520, the AMS Committee shall call and hold closed sessions when reviewing or discussing SSI. Only those members who have been determined to have a "need to know" the particular SSI to be discussed shall be admitted to the closed session:

2. Calling Closed Sessions. Closed sessions shall be noticed on the agenda. To the greatest extent possible, the standardized agenda descriptions consistent with 49 CFR part 1520.7 shall be used. Prior to holding a closed session, the AMS Committee shall convene in open session and provide an opportunity for general membership comment as to the closed session items.

3. Reports from Closed Session. It is the policy that each AMS Committee meeting holding a closed session will inform the public to the greatest extent possible of action taken in closed session. However, the need for confidentiality is inherent in closed sessions and revelation of certain matters may be detrimental to the legitimate goals and responsibilities of the AMS Committee. Accordingly, only a representative designated by the Chairman shall be authorized to make approved reports regarding closed sessions.
4. Disclosure of Security Sensitive Information. Before any individual or entity is provided SSI, the individual or entity representative shall be required to execute a non-disclosure agreement. The Executive Secretary shall ensure that records containing SSI are appropriately marked SSI and protected from release under the FOIA.
5. Protection of SSI from FOIA requests. Wherever practical, SSI shall be redacted from records otherwise subject to disclosure under FOIA. If it is impractical to redact SSI from a record otherwise subject to disclosure, the entire record shall be exempt from disclosure.
6. Security Clearances. It is not anticipated that committee members will have a need to discuss classified information. However, if a need arises, the Chairperson may request security clearances for those committee members with whom the classified information will be discussed. In accordance with reference (b), by using the definition of "employee" under Executive Order 12968, the Coast Guard is permitted to sponsor and grant clearances for a select number of committee members. Requests for clearances will be prepared by the Executive Secretary and will be submitted to Commandant (G-MPS) for approval.

Approved 30 January 2004.

//s//  
Frank M. Paskewich  
Captain, U.S. Coast Guard  
Inland Waterways Coordinator /  
Chairman, Western Rivers Area Maritime Security Committee  
By direction of the Commander,  
Eighth Coast Guard District

**2310 Committee Structure and Procedural Rules**

Refer to Section 2300 (Western Rivers Area Maritime Security Committee Charter). Appendix 9100 is a listing of the Chairperson, Vice Chairperson, Executive Secretary and Executive Steering Committee members.

**2320 Relationship to Other Committees**

(a) Each FMSC under this plan has established one or more AMS subcommittees to address issues particular to their area of responsibility. These subcommittees (referred to in this plan as “local AMS Committees”, “FMSC AMS Committees”, or simply “AMS Committees”) are organized and perform the functions as detailed in 33 CFR 103.300, however, specific membership requirements listed in sections 103.305(b) and 103.305(c) are waived. The local AMS Committees will be chartered in each FMSC Annex to this plan.

(b) The WR AMS Committee encompasses the local AMS Committees and provides for coordination and consistency throughout the region. Each AMS committee shall work with adjoining FMSC zones’ committees to ensure consistency and resolve any conflicts in plan implementation.

**3000 AWARENESS****3100 Introduction**

(a) The AMS Plan is intended to be the fundamental element in building vigilant situational awareness, and is key to the successful development of a maritime domain awareness program. It serves to assist the United States Department of Homeland Security (DHS) in producing a common operational picture of the maritime environment. The AMS Plan affords critical decision makers within each FMSC zone rapid access to vital information during routine and crisis maritime situations.

(b) The WR and FMSC AMS Committees are good forums for use by all levels of government to distribute information about MHS issues. Local, state, and federal governments will use established public awareness procedures in addition to presenting information to the AMS Committees and other regional public committees. AMS Committees are also good forums for use by the private sector for bringing security issues to the attention of the government and other members of the private sector. AMS Committees reserve the right to implement additional public awareness activities, as they feel necessary or prudent.

**3200 Federal, State & Local Security & Law Enforcement Agency Jurisdiction**

(a) Each FMSC Annex under this plan will list federal, state and local security and law enforcement jurisdictional boundaries and areas of responsibility. These agencies should be organized in a three-tiered response system as noted below. A description of each agency’s individual location and capability will greatly enhance the Committee’s ability to determine which resources with what capacities, and how many of each, may respond to a TSI.

(b) Agencies are tiered as follows:

- (1) Tier 1 agencies are those such as police, fire and emergency medical units who are normally dispatched thru the emergency 911-call system (First Responders).
  - (2) Tier 2 agencies are those with special response, recovery and containment capabilities for dealing with hazardous materials, rough terrain or underwater search and recovery, and other agencies having excavation or heavy equipment capabilities.
  - (3) Tier 3 agencies include the National Guard, military reserve, and other national or state level response elements (resources requiring federal or state activation).
- (c) Primary agency responsibilities:
- (1) The United States Coast Guard (USCG), using its authorities under U.S. law and International treaty, has the lead responsibility for the implementation and oversight of security plans and crisis management in, on, under, or adjacent to navigable waterways. This includes participation in the WR and local AMS Committees for development, maintenance, and implementation of the AMS Plan. The USCG may provide shoreside, afloat, and airborne resources to conduct routine patrols of the region.
  - (2) The Federal Emergency Management Agency (FEMA) is responsible for maintaining the Federal Response Plan (FRP) and National Response Plan (NRP) and coordinating federal consequence management activities.
  - (3) The Federal Bureau of Investigation (FBI), using its authorities under U.S. law, is responsible for the implementation and oversight of security and crisis management during terrorist incidents. In the event of a maritime incident, the FBI and USCG will coordinate response efforts.
  - (4) U.S. Army Corps of Engineers (ACOE), in conjunction with the FMSC, is responsible for maintaining waterways infrastructure, including locks and dams. In the event of a maritime incident they will implement internal security measures and coordinate with the FMSC.
  - (5) Each state emergency management agency within the region is responsible for maintaining the state emergency services' plans and coordinating state consequence management activities with local jurisdictions.
  - (6) Local law enforcement (LE) agencies within the region, using their authorities under state and local laws, are responsible for normal LE duties and response to reported security breaches.
  - (7) Local emergency service providers within the region, using their authorities under state and local laws, are responsible for first responder actions and damage assessments.
- (d) Where a Geographic Information System (GIS) already exists, it is recommended that separate agency jurisdictional boundaries be portrayed on maps or charts in an overlay fashion. If possible, the portrayal will extend outside the AMS Committee's FMSC zone to reveal other neighboring agencies or elements that may be involved in both routine and crisis situations.

**3210 Inland River Vessel Movement Center**

The Coast Guard has established the Inland River Vessel Movement Center (IRVMC) in St. Louis, MO to maintain tracking data on all barges in the western rivers region carrying Certain Dangerous Cargoes (CDC) as defined in 33 CFR 160.204. This information is provided to the FMSCs for use in maintaining Maritime Domain Awareness (MDA) and to develop security operations strategies. The IRVMC may be contacted by toll-free telephone at (866) 442-6089, by fax at (866) 442-6107, or by email at [irvmc@cgstl.uscg.mil](mailto:irvmc@cgstl.uscg.mil). Additional information is available on the IRVMC website at [www.uscg.mil/d8/divs/m/IRVMC.htm](http://www.uscg.mil/d8/divs/m/IRVMC.htm).

**3300 Area Maritime Security (AMS) Assessment**

(a) This AMS Plan is prepared based on an AMS Assessment, which is a risk-based analysis of the port or ports, and considered the nine items listed in 33 CFR 103.405(b)(1)-(9). The WR AMS Committee assessed assets common to all ports in the region, while FMSC committees focused on unique features in their ports. The Coast Guard has developed a process that consists of five steps more fully outlined in enclosure (3) to Navigation and Vessel Inspection Circular (NVIC) 9-02 Change 1.

(b) The steps are:

- (1) Identify critical operations and infrastructure.
- (2) Develop attack scenarios.
- (3) Conduct consequence and vulnerability assessments for each scenario.
- (4) Categorize and prioritize scenarios.
- (5) Develop mitigation strategies.

**3310 Maritime Security Assessment Report**

(a) An initial Area Maritime Security Assessment has been completed for all FMSC zones using the Coast Guard's Port Security Risk Assessment Tool (PSRAT). The results of this assessment have been shared with the AMS Committees under each FMSC and used in the development of the FMSC Annexes to this plan.

(b) The Port Security Risk Assessment Tool (PSRAT) was first conducted by Coast Guard personnel in November 2001, and was updated periodically to refresh infrastructure information as or as new versions of the tool became available. The PSRAT identified all designated waterfront facilities, crossing infrastructure (including power lines, bridges, tunnels, and pipelines), waterway systems, certain non-designated waterfront facilities, and certain vessels. A series of scenarios were developed for vulnerable infrastructure, and consequences were identified for each target-scenario combination. Conducting the PSRAT assisted the FMSCs in identifying and assessing physical security needs for infrastructure and operations in the ports, structures considered critical for continued operation of the port, existing security systems and equipment available to protect maritime personnel, relevant transportation infrastructure, and utilities.

(c) The WRAMSPC identified potential threat and attack scenarios for targets or target classes, based on realistic and known capabilities and intentions as evidenced by

past events and available intelligence. Each target/attack scenario combination was evaluated in terms of the potential consequences of the attack and the vulnerability of the target to the attack. Scenarios that require mitigation strategies based on the consequence and vulnerability assessment are considered “Most Probable TSIs” and are discussed in Section 5300.

(d) Each FMSC will maintain the assessment data (PSRAT) for their AOR and make the information available to their AMS Committees as needed for plan development and resource coordination.

(e) Sections 4320, 4420, and 4520 provide risk reduction strategies at each of the MARSEC levels.

(f) The AMS Assessment for each FMSC zone is designated SSI and must be protected in accordance with 49 CFR 1520.

### **3400 Communications**

(a) Effective communication is vital to pre- and post incident response. An understanding of communication methodology, programs, processes, and physical attributes is essential to all personnel involved in the security process.

(b) The local AMS Committee charters identify how and when the committees will meet, which may include providing advice or assistance to the FMSC in the communication of security information.

(c) Redundant methods for communicating vital information to appropriate facilities, vessels, maritime stakeholders, and recreational boaters may include:

- (1) Telephone
- (2) Facsimile
- (3) Broadcast Notice To Mariners (BNTM)
- (4) Urgent Marine Information Bulletins (UMIB)
- (5) Email
- (6) Dissemination through AMS Committee/industry representatives
- (7) Posting on appropriate websites
- (8) Announcement on state Emergency Alert Systems
- (9) Notification of state Emergency Management Agency (EMA), Emergency Operations Center (EOC) or other appropriate agency
- (10) Site visits

### **3410 Communication of Security Information**

(a) Security informational needs are multi-layered with a large variety of stakeholder requirements. Notifications to Federal, state, and local enforcement agencies (e.g. local FBI Field Offices, Joint Terrorism Task Force (JTTF) and/or Anti Terrorism Advisory Council (ATAC), State Police) may be a necessary primary response to a security threat.

(b) When the FMSC is made aware of a threat that may cause a transportation security incident, the FMSC will, when appropriate, communicate to the port stakeholders, vessels, and facilities in his or her AOR the following details:

- (1) Geographic area potentially impacted by the probable threat.
- (2) Any appropriate information identifying potential targets.
- (3) Onset and expected duration of probable threat.
- (4) Type of probable threat.
- (5) Required actions to minimize risk.

(c) Section 3500 of this plan contains information pertaining to the protection and dissemination of Sensitive Security Information (SSI).

(d) Tabs A, B and C provide guidance on communicating security information and reports.

#### **3410.1 Communication With the Public**

(a) The public as a whole must be notified of possible actions or operations that might affect it. There are a variety of systems that may be used to communicate information on restrictions, closures, and activities that are exclusionary or restrictive in nature, including the Emergency Broadcast System, Community Awareness and Emergency Response (CAER) network, press releases, and State and local emergency management offices.

(b) FMSCs must appropriately disseminate cleared threat information directly to State, local, or private sector officials in accordance with DHS and Coast Guard policy. That policy requires organizations within the DHS to communicate threats outside of DHS through the Information Analysis and Infrastructure Protection (IAIP) Directorate. As such, the Secretary of DHS, or his approved designee, will approve all analytical conclusions involving threats of terrorism or WMD prior to dissemination to State, local, or private sector officials. The policy permits direct communication if the Commandant or his designees (FMSCs) determine that exigent circumstances require communication to prevent, preempt, or disrupt an imminent threat.

(c) Each FMSC Annex contains specific means for communications during emergency and non-emergency situations.

#### **3410.2 Communications With Waterway Users**

(a) Communicating security information to waterway users will include many of the processes currently used to identify hazards to navigation or safety related concerns of the MTS. The specific methods that could be used to communicate to waterway users include Notice to Mariners, navigation publications, marine exchanges, vessel traffic services, and State and local threat warning systems.

(b) Each FMSC Annex contains specific means for communications during emergency and non-emergency situations.

#### **3410.3 Communications With Commercial Vessels**

(a) Communicating with commercial vessels will be accomplished primarily through BNTMs, voice or electronic communication with the Company Security Officer or Vessel Security Officer (CSO or VSO), and/or relaying information through ACOE lock operators or the IRVMC. Each FMSC shall maintain a list of CSOs responsible for the vessels within their fleet of responsibility including 24-hour contact information.

(b) CSOs/VSOs shall ensure that all vessels operating in the affected area are notified of the security information and acknowledgement of receipt is provided to the FMSC. Security information must be communicated in accordance with Section 3500.

(c) Section 4210 details the communications required between a facility and any vessels arriving that are at a different MARSEC Level.

#### **3410.4 Communications With Facilities**

(a) Communication of security information with regulated and non-regulated facilities within the WR AMS Committee's AOR will be undertaken using prearranged methods and procedures identified in individual FMSC Annexes to this plan. Each FMSC shall maintain a list of Facility Security Officers (FSOs) responsible for the regulated facilities within their FMSC zone including 24-hour contact information.

(b) FSOs shall ensure that all facilities operating in the affected area are notified of the security information and acknowledgement of receipt is provided to the FMSC. Security information must be communicated in accordance with Section 3500.

#### **3410.5 Communicating with Companies**

See section 3410.3 above.

#### **3410.6 Role of the Area Maritime Security Committee**

(a) The AMS Committee's role in communicating security information and procedures is pivotal to ensuring that security information can be quickly and effectively transmitted to a broad range of audiences.

(b) The AMS Committee shall serve as a link for communicating threats and changes in MARSEC Levels and disseminating appropriate security information to port stakeholders. As such, the committee may be convened to advise and assist the FMSC in the communication of security information. Some instances where this may be necessary include:

- (1) Identify requirements that will need to be implemented from the AMS Plan when notified of an increase in threat.
- (2) Identify requirements that will need to be implemented from the AMS Plan when notified of a MARSEC Directive.
- (3) Communicate threat information through prearranged procedures to MTS/waterway users.
- (4) To convene a lessons learned/hot wash session to develop measurement and improvement strategies after communication portions of the plan have been implemented.

#### **3420 Security Reporting**

The National Response Center (NRC) will act as the fusion center for all security information required by 33 CFR 101.305, and serve as a conduit of information to and from consequence mitigation and law enforcement organizations. This includes reports of suspicious activity and actual security breaches that do not result in a TSI, which normally will require simultaneous notification to local law enforcement

authorities. In addition, facilities or individuals may contact the FMSC directly with such information. FMSCs receiving information from entities subject to Subchapter H of Chapter I of 33 CFR will advise the reporting entities of their responsibilities under the regulations to notify the NRC. Entities non subject to the aforementioned regulations will be highly encouraged to report information to the NRC. In all cases the FMSC will confirm with the NRC that notification was made. FMSCs will assure that relevant information is recorded in unit logs and that notification is made to appropriate local agencies by the FMSC Staff. The reports and information garnered as a result of follow-on investigations will formulate intelligence and threat information that can be used to adjust security conditions throughout the country. Procedures for reporting a Transportation Security Incident are in Section 5210. TAB C includes forms that can be used for security reports of suspicious behavior and breaches of security.

### **3420.1 Procedures for reporting suspicious activity**

- (a) Quick Response Cards (QRC), located in Tab C, may be used as an effective and efficient tool to collect important information, including reports of suspicious activities, during periods of heightened awareness, security breaches, and potential or actual TSIs. When used properly, the QRC eliminates confusion and ensures all necessary information is captured. The subject matter covered, or title, may be kept general, but specificity should be included in the body of the document. The sample QRCs in Tab C will be modified to include appropriate local contact information.
- (b) Local authorities (911 or other emergency response contact) should be notified for any activities that pose an immediate threat to persons or property.
- (c) Facilities and vessels regulated under 33 CFR Parts 104 or 105 must, and all other port entities are strongly encouraged to, report all suspicious activities to the **National Response Center (NRC)** via one of the following:
  - (1) Toll free telephone: 1-800-424-8802
  - (2) Direct telephone: 202-267-2675
  - (3) Fax: 202-267-2165
  - (4) Telephone Device for the Deaf (TDD): 202-267-4477
  - (5) Email: [lst-nrcinfo@comdt.uscg.mil](mailto:lst-nrcinfo@comdt.uscg.mil)
- (d) In addition to notifying the NRC, all suspicious activities should be reported directly to the FMSC.
- (e) Callers shall be prepared to provide as much of the following information as possible:
  - (1) Their own name and contact information
  - (2) The name and contact information of the suspicious or responsible party
  - (3) The location of the incident, as specifically as possible
  - (4) The description of the incident or activity involved

**3420.2 Procedure for Reporting Breaches in Security**

Same as Section 3420.1

**3430 MARSEC Directives**

(a) MARSEC Directives permit the Coast Guard to provide sensitive security information to the maritime industry while protecting it from full public disclosure. As provided in 33 CFR 101.405, the Coast Guard may issue MARSEC Directives that provide vessels and facilities nationwide with mandatory security measures in the form of objective performance standards related to such security concerns as access control and handling of cargo. By designating MARSEC Directives as SSI, the Coast Guard may communicate objective performance standards to specific individuals or entities without subjecting the information to full public disclosure.

(b) MARSEC Directives also allow the Commandant of the Coast Guard to ensure consistency among FMSCs as they enforce the provisions of the MTSA in their individual zones. Additionally, MARSEC Directives allow the Coast Guard flexibility in tailoring objective performance standards to the prevailing threat environment or industry segment.

(c) MARSEC Directives do not impose new requirements, but provide direction to the industry on how to meet the performance standards already required by the MTSA. The directives will only be issued by Commandant, and only after consultation with other interested Federal agencies within the Department of Homeland Security.

**3430.1 Procedures for Communicating MARSEC Directives**

(a) When a new MARSEC Directive is issued, the Coast Guard will publish a notice in the Federal Register and announce through other means (e.g., local Notices to Mariners, and press releases) that it has issued a new MARSEC Directive.

(b) The MARSEC Directives will be individually numbered, and will be assigned to a series that corresponds with the Part of 33 CFR subchapter H to which the MARSEC Directive refers. For example, the first MARSEC Directive addressing a new requirement for vessels regulated under Part 104 of 33 CFR subchapter H would be identified as “MARSEC Directive 104-01.”

(c) Upon receiving notice that a new MARSEC Directive has been issued, the FMSC will contact affected entities in their zone or Fleet of Responsibility to arrange delivery of the MARSEC Directive. The FMSC or District Commander will confirm, prior to distributing the MARSEC Directive, that the requesting entity is a “Covered Person” with a “need to know.” The requesting entity must confirm to the FMSC through the use of a standard non-disclosure form that it will safeguard the MARSEC Directive as SSI. The FMSC will maintain a record of all persons receiving a MARSEC Directive. A standard non-disclosure form is provided in TAB D.

(d) FMSCs will process MARSEC Directives in accordance with the following general procedures:

- (1) Develop list of affected entities for approval by the FMSC.

(2) Contact affected entities to arrange delivery or pickup of the MARSEC Directive.

(3) Assure that SSI non-disclosure agreements are on file or executed prior to providing the MARSEC Directive.

(4) Document receipt of the MARSEC Directive by signature of the recipient.

(5) Verify compliance with the MARSEC Directive in accordance with unit procedures.

(6) Conduct follow-up as necessary.

### **3430.2 Procedures for Responding to MARSEC Directives**

(a) Once a MARSEC Directive has been issued, it is the responsibility of the affected entities to confirm compliance with the Directive to the local FMSC and specify the methods by which the mandatory measures in the directive have been, or will be, met.

(b) The FMSC will at the time of issuance of the MARSEC Directive establish the procedures and timeframes to be followed in providing notice of compliance. Acceptable means of notification include telephone, e-mail, fax, or in person. The FMSC's staff will verify that all affected entities have reported compliance, and will verify compliance through targeted inspections of the affected entities.

(c) In some cases, recipients may elect to submit proposed equivalent security measures to the local FMSC. Section 7300 details procedures to ensure compliance with MARSEC Directives and other requirements. Requests for equivalent security measures or waivers will be handled in accordance with 33 CFR Part 101.130, as noted in Section 4220. The FMSC will at the time the request for equivalent security measure or waiver is received establish the procedures and timeframe for acting on the request, will designate a member of the FMSC's staff to serve as the point of contact for the requestor, and will establish a mutually agreed means of notifying the requestor when a decision has been made.

### **3430.3 Role of the Area Maritime Security (AMS) Committees**

(a) 33 CFR 103.310 directs the AMS Committees to serve as a link for communicating threats and changes in MARSEC Levels, and disseminating appropriate security information to port stakeholders. Accordingly, the FMSC may from time to time and to different degrees, require the AMS Committee to assist in the distribution of MARSEC Directives.

(b) In anticipation of providing assistance in the distribution of MARSEC Directives, the WRAMS Committee and FMSC Subcommittees should develop local protocols and procedures addressing how they will assist in ensuring that directives are distributed and received in a timely manner, and the means by which they will interface with their respective industry representatives.

(c) In general each member of the WRAMS Committee and each member of the FMSCs' AMS Subcommittees will serve as a point of contact for their respective agencies or segments of the maritime industry. Members will conduct outreach to

assure that agencies, organizations and industries are aware of the MARSEC Directive, that they are engaged with the FMSCs to obtain copies of it, and that they understand their obligations to comply and report compliance. Appropriate means of communicating with industries include telephone, e-mail, fax, in person visits, and industry websites.

#### **3440 MARSEC Levels**

(a) The Coast Guard has developed a three-tiered system of MARSEC Levels consistent with the DHS Homeland Security Alert System (HSAS). The three-level MARSEC system is separate from, yet used in conjunction with, the HSAS system. MARSEC Levels will be set based on maritime interests and may not always correlate to the HSAS. The international community is also using a three-tiered alert system that is consistent with the MARSEC levels used by the Coast Guard.

(b) MARSEC Levels were designed to provide a means to easily communicate pre-planned scalable responses to increased threat levels. MARSEC Levels will normally be set commensurate with the HSAS. Because of the unique nature of the maritime industry, the HSAS threat conditions and MARSEC Levels will align closely, though they will not directly correlate:

(1) MARSEC Level 1 corresponds to HSAS Threat Conditions Green, Blue, and Yellow. It is the level for which minimum appropriate protective security measures shall be maintained at all times.

(2) MARSEC Level 2 corresponds to HSAS Threat Condition Orange. It is the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident.

(3) MARSEC Level 3 corresponds to HSAS Threat Condition Red. It is the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable or imminent, although it may not be possible to identify the specific target.

(c) The Secretary of the DHS sets the HSAS threat condition and only the Commandant will have the authority to change MARSEC Levels to match the HSAS. An exception is provided, which allows an FMSC to temporarily raise the MARSEC Level in his/her FMSC zone to address a threat to the MTS when the immediacy of the threat or incident does not allow time to notify the Commandant.

(d) FMSCs will only exercise this authority under the most urgent circumstances. Such circumstances would include an incident where immediate action to save lives or mitigate significant property or environmental damage that would result in a TSI is required, and timely prior notification to the Commandant is not possible. If such a circumstance does arise, the FMSC must inform the Commandant via the chain of command as soon as notification is possible. The heightened MARSEC Level will continue only as long as necessary to address the threat which prompted raising the level.

(e) MARSEC changes will be triggered under limited circumstances and usually in conjunction with elevation of HSAS levels, such as when the threat that prompted a

change in the HSAS Threat Condition also imperils a component of the MTS. However, there will also be instances where the HSAS Threat Condition is elevated for threats unrelated to the MTS, or where, after the HSAS Threat Condition is elevated, it becomes clear that the MTS is not a target. In these instances, the Commandant may set MARSEC Levels below the equivalent HSAS Threat Condition. Furthermore, the Commandant may choose to raise the MARSEC Level at only specific ports in response to the elevated HSAS Threat Condition instead of requiring all ports nationwide or on a particular coast to elevate their protective measures. An example of where this might occur includes ports where military load-outs occur or at ports that are considered strategically important.

#### **3440.1 Procedures to Communicate Changes in MARSEC Levels**

(a) Because of the uniqueness of ports and their operations, the AMS Committee may choose a particular means of communication or a combination of means to inform all port users that there has been a change in the MARSEC Level. Section 3410 lists means of communicating this information. Changes in MARSEC Levels are not considered SSI and can be disseminated by any means available.

(b) Each FMSC shall ensure all companies, facilities and vessels in their fleets of responsibility that are required to have a security plan are notified of changes in MARSEC levels. Notification will be made through direct contact by the FMSC staff with CSOs, FSOs, and VSOs. In addition, public announcements will be made using the means identified in paragraph (c) below.

(c) The specific means of communicating changes in MARSEC Levels in each FMSC zone are as follows:

- (1) Telephone
- (2) Facsimile
- (3) Broadcast Notice To Mariners (BNTM)
- (4) Urgent Marine Information Bulletins (UMIB)
- (5) E-mail
- (6) Dissemination through AMS Committee/industry representatives
- (7) Posting on appropriate websites
- (8) Announcement on state Emergency Alert Systems
- (9) Notification of state Emergency Management Agency (EMA), Emergency Operations Center (EOC), or other appropriate agency.
- (10) Site visits

#### **3440.2 Notification of MARSEC Level Attainment**

Vessels and facilities regulated under 33 CFR Parts 104 and 105 must comply, within 12 hours of receiving notification of a change in MARSEC Level, with the required additional security measures in accordance with their plan. A report of compliance (or noncompliance) shall be made to the FMSC via telephone or electronic means. Section 7300 details procedures to ensure compliance with MARSEC Directives and other requirements.

(e) FMSCs will verify MARSEC Level attainment using the following general procedures:

(1) Within the 12-hour notification period FMSCs will continuously document notifications on the list of affected entities. Notifications may be made by telephone, e-mail, fax, or in person.

(2) After the 12-hour notification period the FMSCs will initiate contact with entities that have not confirmed attainment of the MARSEC Level. If attainment cannot be verified the FMSC will dispatch a representative to visit the entity to ensure that attainment has occurred.

(3) Non-attainment will be dealt with through the control procedures specified in 33 CFR 101.410.

(4) The FMSC will conduct spot-checks of random facilities and vessels, or targeted compliance inspections of select facilities and vessels to verify compliance.

(5) Follow-up will be conducted as necessary.

### **3440.3 Role of Area Maritime Security (AMS) Committee**

The AMS Committee may assist the FMSC in the communication of changes of the MARSEC Level. The AMS Committee may also assist in the development of protocols or procedures that ensure attainment notifications are received in a timely manner.

### **3500 Sensitive Security Information**

This section governs the maintenance, safeguarding, and disclosure of AMS Plan information, and other records and information, that have been designated as Sensitive Security Information (SSI), as defined in paragraph 3510 of this plan. This section does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is exempt from public disclosure under the Freedom of Information Act (FOIA), or other applicable law and regulations.

#### **3510 Information Designated as Sensitive Security Information**

(a) In general. In accordance with 49 CFR 1520.3, SSI is information obtained or developed while conducting security activities, including research and development, when it has been determined that disclosure would:

(1) Constitute an unwarranted invasion of privacy (including, but not limited to information contained in any personnel, medical, or similar file);

(2) Reveal trade secrets or privileged or confidential information obtained from any person; or

(3) Be detrimental to the to the safety of persons traveling in transportation.

(b) Information constituting SSI. Except as otherwise provided, in the interest of public safety or in furtherance of transportation security, the following information and records containing such information constitute SSI:

- (c) Security programs and contingency plans. Any security program or security contingency plan issued, established, required, received, or approved by DHS, including:
- (1) Any vessel, maritime facility, or port area security plan required or directed under Federal law;
  - (2) Any national or area security plan prepared under 46 U.S.C. 70103; or
  - (3) Any security incident response plan established under 46 U.S.C. 70104.
- (d) Security Directives. Any Security Directive or order:
- (1) Issued by the Transportation Security Administration (TSA) under 49 CFR §§ 1542.303 or 1544.305, or other authority;
  - (2) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR Part 6, or 33 U.S.C. 1221 et seq. related to maritime security; or
  - (3) Any comments, instructions, and implementing guidance pertaining thereto.
- (e) Information Circulars. Any notice issued by DHS regarding a threat to maritime transportation, including:
- (1) Any Information Circular issued by TSA under 49 CFR §§ 1542.303, § 1544.305, or other authority; or
  - (2) Any Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.
- (f) Performance specifications. Any performance specification and any description of a test object or test procedure, for:
- (1) Any device used by the Federal Government or any other person pursuant to any MTS requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; or
  - (2) Any communications equipment used by the Federal Government or any other person in carrying out or complying with any MTS requirements of Federal law.
- (g) Vulnerability assessments. Any vulnerability assessment directed, created, held, funded, or approved by the DHS, or that will be provided to DHS in support of a Federal security program.
- (h) Security inspection or investigative information. Details of any security inspection, or investigation of an alleged violation of MTS requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.
- (i) Threat information. Any information held by the Federal Government concerning threats against transportation or transportation systems, and any sources or methods used to gather or develop threat information, including threats against cyber infrastructure.

(j) Security measures. Specific details of MTS measures, both operational and technical, whether applied directly by the Federal Government or another person, including:

- (1) Security measures or protocols recommended by the Federal Government;
- (2) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security activities, to the extent it is not classified national security information.

(k) Security screening information. The following information regarding security screening under MTS requirements of Federal law:

- (1) Any procedures, including selection criteria, and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo conducted by the Federal Government or any other authorized personnel;
- (2) Any information or sources of information used by a passenger or property screening program or system, including an automated screening system;
- (3) Detailed information about locations at which particular screening methods or equipment are used;
- (4) All security screener tests and scores of such tests;
- (5) Performance or testing data from security equipment or screening systems;
- (6) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

(l) Security training materials. Records created or obtained for the purpose of training persons employed by, contracted with, or acting for the Federal Government or another person to carry out any MTS measures required or recommended by DHS.

(m) Identifying information of certain transportation security personnel. Lists of the names or other identifying information that identify persons as:

- (1) Having unescorted access to a secure area or restricted area of a maritime facility, port area, or vessel;
- (2) Holding a position as a security screener employed by or under contract with the Federal Government pursuant to MTS requirements of Federal law; or
- (3) Holding a position with the Coast Guard responsible for conducting vulnerability assessments, security boarding teams, or engaged in operations to enforce maritime security requirements or conduct force protection.

(n) Critical maritime infrastructure asset information. Any list identifying systems or assets, whether physical or virtual, so vital to the maritime transportation system that the incapacity or destruction of such assets would have a debilitating impact on transportation security, if the list is:

- (1) Prepared by DHS; or

- (2) Prepared by a State or local government agency and submitted by the agency to DHS.
- (o) Systems security information. Any information involving the security of operational or administrative data systems operated by the Federal Government that have been identified by the DHS as critical to maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.
- (p) Confidential business information.
- (1) Solicited or unsolicited proposals received by DHS, and negotiations arising from the same, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to MTS measures;
- (2) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS in carrying out MTS responsibilities; and
- (3) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS in carrying out MTS responsibilities, but only if the source of the information does not customarily disclose it to the public.
- (q) Research and development. Information obtained or developed in the course of research related to MTS activities, where such research is approved, accepted, funded, recommended, or directed by the DHS, including research results.
- (r) Other information. Any information not otherwise described in this section that the DHS determines is SSI under 49 U.S.C. 114(s). Upon the request of another Federal agency, the DHS may designate information as SSI not otherwise described in this section.

### **3520 Covered Persons**

“Covered Person” means any organization, entity, individual, or other person described in paragraph 3520.1, *infra*. In the case of an individual, Covered Person includes any individual applying for employment in a position that would allow designation as a Covered Person, or in training for such a position, regardless of whether that individual is receiving a wage, salary, or other form of payment. Covered Person includes a person applying for certification or other form of approval that, if granted, would make the person a Covered Person described in 3520.1, *infra*.

#### **3520.1 Designation as a Covered Person**

- (a) The following may be designated as a Covered Person:
- (1) Every owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators required to have a security plan under Federal or international law;

- (2) Every owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act, (Pub.L. 107-295), 46 U.S.C. 70101 et seq., 33 CFR Part 6, or 33 U.S.C. 1221 et seq.;
- (3) Any person performing the function of a computer reservation system or global distribution system for cruise line passenger information;
- (4) Any person participating in the National or an area security committee established under 46 U.S.C. 70112, or a Port Security Committee;
- (5) Any industry trade association that represents Covered Persons and has entered into a non-disclosure agreement (TAB D) with the DHS;
- (6) DHS;
- (7) Any person conducting research and development activities that relate to MTS and are approved, accepted, funded, recommended, or directed by DHS;
- (8) Any person who has access to SSI, as specified in paragraph 3540;
- (9) Each person employed by, contracting with, or acting for a Covered Person, including a grantee of DHS, and including a person formerly in such position;
- (10) Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the DHS, or that has prepared a vulnerability assessment that will be provided to DHS in support of a Federal security program;
- (11) Each person receiving SSI under paragraph 3540.

### **3530 Restrictions on the Disclosure of SSI**

(a) Duty to protect information. A Covered Person must:

- (1) Take reasonable steps to safeguard SSI in that person's possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it in a secure container, such as a locked desk or file cabinet or in a locked room;
- (2) Disclose or otherwise provide access to SSI only to Covered Persons who have a "need to know", unless otherwise authorized in writing by the Commandant of the Coast Guard, or the Secretary of DHS;
- (3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DHS;
- (4) Mark SSI as specified in paragraph 3550; and
- (5) Dispose of SSI as specified in paragraph 3580.

(b) Unmarked SSI. If a Covered Person receives a record containing SSI that is not marked as specified in paragraph 3550, the Covered Person must:

- (1) Mark the record as specified in paragraph 3550; and
- (2) Inform the sender of the record that the record must be marked as specified in paragraph 3550.

(c) Duty to report unauthorized disclosure. When a Covered Person becomes aware that SSI has been released to unauthorized persons, the Covered Person must promptly inform TSA or the applicable DHS component or agency.

### **3540 Persons with a “Need to Know”**

(a) In general. A person has a “need to know” SSI in each of the following circumstances:

- (1) When the person requires access to specific SSI to carry out MTS activities approved, accepted, funded, recommended, or directed by DHS;
- (2) When the person is in training to carry out MTS activities approved, accepted, funded, recommended, or directed by DHS;
- (3) When the information is necessary for a person to supervise or otherwise manage individuals carrying out MTS activities approved, accepted, funded, recommended, or directed by the DHS;
- (4) When the person needs the information to provide technical or legal advice to a Covered Person regarding MTS requirements of Federal law;
- (5) When the person needs the information to represent a Covered Person in connection with any judicial or administrative proceeding, except in the case of an individual serving as litigation counsel who is not a direct employee of the Covered Person, the person has a “need to know” only if:
- (6) In the judgment and sole discretion of the DHS, access to the SSI is necessary for adequate representation of the Covered Person in the proceeding. The DHS may make the individual’s access to the SSI contingent upon satisfactory completion of a security background check, and the imposition of a protective order, or agreed upon procedures that establish requirements for safeguarding SSI and that are satisfactory to the Secretary of DHS.

(b) Federal employees, contractors, and grantees.

- (1) A Federal employee has a “need to know” SSI if access to the information is necessary for performance of the employee’s official duties.
- (2) A person acting in the performance of a contract with or grant from DHS has a “need to know” SSI if access to the information is necessary to performance of the contract or grant.

(c) “Need to know” further limited by the DHS. DHS may make a finding that only specific persons or classes of persons have a “need to know specific SSI.”

### **3550 Marking SSI**

(a) Marking of paper records. In the case of paper records containing SSI, a Covered Person must mark the record by placing the protective marking conspicuously on the top, and the distribution limitation statement on the bottom of:

- (1) The outside of any front and back cover, including a binder cover or folder, if the document has a front and back cover;
- (2) Any title page; and

(3) Each succeeding page of the document that contains SSI.

(b) Protective marking. The protective marking is: SENSITIVE SECURITY INFORMATION. The marking must be applied to all documents that contain SSI. This marking should be written or stamped in plain style bold type, Times New Roman and a font size of 16, or an equivalent style and font size.

(c) Distribution limitation statement. The distribution limitation statement is:

**WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this record may be disclosed to persons without a “need to know,” as defined in 49 CFR 1520.5, except with the written permission of the Secretary of Homeland Security. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR Part 1520.**

(d) Other types of records. In the case of non-paper records that contain SSI, including motion picture films, videotape recordings, audio recording, and electronic and magnetic records, a Covered Person must clearly and conspicuously mark the records with the protective marking and the distribution limitation statement such that the viewer or listener is reasonably likely to see or hear them when obtaining access to the contents of the record.

### **3560 SSI Disclosed By or To the Coast Guard**

(a) In general. Except as provided in paragraphs (b) through (e) of this section, and notwithstanding the Freedom of Information Act (5 U.S.C. 552), the Privacy Act (5 U.S.C. 552a), and other laws, records containing SSI are not available for public inspection or copying, nor does DHS release such records to persons without a “need to know.”

(b) Disclosure under the Freedom of Information Act and the Privacy Act. If a record contains both SSI and information that is not SSI, the Coast Guard, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.

(c) Disclosures to committees of Congress and the General Accounting Office. Nothing in this part precludes the Coast Guard from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

(d) Disclosure in enforcement proceedings.

(1) In general. The Coast Guard may provide SSI to a person in the context of an administrative enforcement proceeding when, in the sole discretion of the DHS or the Commandant of the Coast Guard, as appropriate, access to the SSI is necessary for the person to prepare a response to allegations contained in a legal enforcement action document issued by the Coast Guard.

(2) Obligation to protect information. When an individual receives SSI pursuant to paragraph (d)(1) of this section, that individual becomes a Covered Person

under paragraph 3520.1 and is subject to the obligations of a Covered Person under this part.

(3) No release under FOIA. When the Coast Guard discloses SSI pursuant to paragraph (d), the Coast Guard makes the disclosure for the sole purpose of providing the information to a person preparing a response to allegations contained in a legal enforcement action document. Such disclosure is not a public release of information under the Freedom of Information Act.

(e) Disclosure in the interest of safety or security. The DHS or the Commandant of the Coast Guard may disclose SSI where necessary in the interest of public safety or in furtherance of transportation security.

### **3570 Consequences of Unauthorized Disclosure of SSI**

Violation of 49 CFR 1520, pertaining to the protection of sensitive security information, is grounds for a civil penalty and other enforcement or corrective action by DHS and appropriate personnel actions for Federal employees.

### **3580 Destruction of SSI**

(a) DHS. Subject to the requirements of the Federal Records Act (5 U.S.C. 105), including the duty to preserve records containing documentation of a Federal agency's policies, decisions, and essential transactions, DHS destroys SSI when no longer needed to carry out the agency's function.

(b) Other Covered Persons.

(1) In general. A Covered Person must destroy SSI completely to preclude recognition or reconstruction of the information (e.g. shredding, burning, pulping) when the Covered Person no longer needs the SSI to carry out transportation security measures;

(2) Exception. Paragraph (b)(1) of this section does not require a State or local government agency to destroy information that the agency is required to preserve under local law.

### **3590 Procedures for Communicating SSI Material.**

(a) SSI material is to be disseminated to AMS Committee members and/or port stakeholders in accordance with the guidance below:

(1) Hard copy dissemination may be accomplished via:

- i) U.S. Mail;
- ii) Intra-office mail; or
- iii) Hand-carrying within/between buildings.

All forms of delivery must be subject to strict packaging and delivery mandates to ensure privacy;

(2) Electronic transmission of SSI may be accomplished via:

- i) Facsimile. The sender must confirm that the facsimile number of the recipient is current and valid and the facsimile machine is in a controlled area where unauthorized persons cannot intercept the SSI facsimile, or the sender

must ensure that an authorized recipient is available at the receiving location to promptly retrieve the information. The information to be transmitted must have a cover sheet that clearly identifies the sender's name and telephone number and contains a warning that, if the message is received by other than the intended recipient, the individual receiving the message must immediately notify the sender for disposition instructions.

ii) Electronic Mail. SSI may be transmitted in an attachment or within the text of an email if it is being sent to Coast Guard workstation email address of a individual determined to have a "need to know". If the email is being sent to any other address, for example ".com", ".gov" or ".net", it must be provided within a password protected document. Zipped files with password protection are considered to meet this requirement. The password may not be contained in the email.

iii) Telephone. The caller must ensure that the person receiving the SSI is an authorized recipient. Individuals needing to pass SSI by telephone will avoid using cellular telephones and cordless telephones unless the circumstances are exigent, or the transmissions are encoded or otherwise protected to reduce the risk of interception and monitoring.

iv) Wireless Devices. The risk of monitoring and interception of SSI is greater when using wireless devices. Therefore, DO NOT use cellular phones, pagers, cordless telephones or personal digital assistants to transmit SSI unless the transmission is encrypted or there is an emergency.

v) Internet. Internet posting of SSI is allowed if the posting is within a secure socket layer (SSL) with minimum access controls, consisting of a user name, and password. The Primary Content Approval Official (PCAOs) is responsible to ensure that no documents/databases containing SSI information are released. In addition, FMSCs may also require SSI warning banners upon logon; electronically signed non-disclosure agreements at each logon; limited user permissions (based on need-to-know) or limitations on storage of SSI information.

### **3600 Maritime Security Training for AMS Plan Implementation**

AMS Committee members are responsible for ensuring that those members of their organizations directly involved in the execution of the AMS Plan are sufficiently trained to execute their roles in implementing the AMS Plan. When standards for maritime security training are developed they will be incorporated into this plan.

### **3700 Security Resources**

Each FMSC Annex to this plan will list the law enforcement agencies with jurisdiction that may be available for response and (if available) their estimated timeframe for dispatch.

**4000 PREVENTION****4100 Introduction**

The FMSCs, in consultation with the AMS Committee, will plan and pre-designate appropriate preventative and protective postures to be assumed according to each MARSEC Level.

**4200 Maritime Security (MARSEC) Level Planning****4210 Procedures When a Vessel and a Facility are at Different MARSEC Levels**

(a) There may be circumstances where a vessel is operating at a higher MARSEC Level than the port or facility that the vessel is calling on. In such cases, the port and its facilities may remain at the existing MARSEC Level. However, if the port or facility is at a higher MARSEC Level per Commandant or FMSC direction, the vessel must attain the corresponding MARSEC Level and notify the FMSC as detailed in section 3440.2.

(b) Since the regulations require the facility to communicate the current MARSEC Level to those vessels at or arriving at its facility, the FSO shall notify the FMSC if a vessel arrives at a lower MARSEC Level. The vessel shall comply without undue delay with all measures for the higher MARSEC level as specified in their vessel security plan or the AMS Plan.

(c) When notified of a vessel arriving at a lower MARSEC Level than its servicing facility the FMSC will take the following steps:

(1) Verify that the facility has notified the vessel that the facility is at a higher MARSEC Level.

(2) Communicate with the vessel to verify its knowledge of the facility's higher MARSEC Level. Such communications may be through the CSO, VSO, FSO, or direct to the vessel using telephone, VHF radio, or a boarding.

(3) Direct the vessel to immediately attain the higher MARSEC Level and to notify the FMSC when in compliance.

(4) At the discretion of the FMSC conduct a boarding of the vessel to verify compliance.

(5) Non-attainment will be dealt with through the control procedures specified in 33 CFR 101.410.

**4220 Requesting Equivalencies and Waivers to MARSEC Directives**

(a) MARSEC Directives will set mandatory measures that all defined entities must meet in a specified time period. These entities will also be required to confirm to the local FMSC receipt of the MARSEC Directive, as well as specify the method by which the mandatory measures have been (or will be) met.

(b) Recipients of MARSEC Directives may elect to submit proposed equivalent security measures to the local FMSC. Section 7300 details procedures to ensure compliance with MARSEC Directives and other requirements. Requests for

equivalent security measures or waivers will be handled in accordance with 33 CFR Part 101.130, as noted in Section 4220. The FMSC will at the time the request for equivalent security measure or waiver is received establish the procedures and timeframe for acting on the request, will designate a member of the FMSC's staff to serve as the point of contact for the requestor, and will establish a mutually agreed means of notifying the requestor when a decision has been made.

(c) 33 CFR 104.130 and 105.130 state that vessel or facility owners or operators may request waivers for any requirement of Parts 104 or 105 that the owner or operator considers unnecessary in light of the nature and operating conditions of the vessel or facility. The request must be submitted in writing to Commandant and include justification as to why the specific requirement(s) are unnecessary for that particular owner's or operator's vessel or facility or its operating conditions. In the case of facilities regulated under 33 CFR 105, the application must be made prior to operating. The Coast Guard will notify the owner/operator when a waiver request is approved or disapproved.

(d) Under 33 CFR 101.420, any person directly affected by a decision or action taken by the FMSC under 33 CFR Subchapter H, may appeal that action or decision to the Eighth Coast Guard District Commander according to the procedures in 46 CFR 1.03-15.

#### **4300 MARSEC Level 1**

##### **4310 Roles, Resources, Authorities, and Responsibilities**

(a) Appropriate federal, state, local and civilian stakeholders shall immediately respond and dispatch appropriate resources to incidents within prescribed timeframes as mandated by their respective agencies. See Sections 3200 and 3700 for general responsibilities and resources of agencies.

(b) The FMSC will coordinate with all port stakeholders to ensure that the port infrastructure is properly assessed, protected and maintained at its normal level of operations. Some of the indicators the FMSC will assess include:

- (1) Public safety
- (2) Extent and impact of waterway closures
- (3) Extent of damage to port infrastructure
- (4) Loss or damage of facilities or commercial goods/services within the port

(c) Civilian stakeholders have developed security plans and mitigation strategies in coordination with the WR and local AMS Committees in accordance with 33 CFR Subchapter H.

(d) Each FMSC Annex will address appropriate stakeholders' responsibilities and jurisdictions.

##### **4320 Standard Security Procedures for MARSEC Level 1**

(a) Each FMSC will review and implement security procedures as necessary given the current threat and official guidance to detect, deter, disrupt, and respond to attacks against the MTS, its operations, and port infrastructure. Vessels and facilities required

to have security plans under 33 CFR Parts 104 and 105 shall follow the security procedures outlined in their approved plan.

(b) Each FMSC Annex will detail specific security procedures and measures for their area.

#### **4330 Physical Security Measures**

(a) Vessels and facilities required to have security plans under 33 CFR Parts 104 and 105 shall implement the security measures outlined in their approved plan. All port entities not covered under Parts 104 and 105 are subject to this plan. Such entities should (and may be required to by a Captain of the Port Order) implement the following recommended security measures (as applicable):

(1) In coordination with the FMSC, plan for and establish Fixed Security Zones and Regulated Navigation Areas (RNAs), and specify who is going to enforce them.

(2) Incorporate security elements into the duties and responsibilities of all port personnel:

i) Define security elements. This may include routine duties, such as observing and reporting malfunctioning security equipment and suspicious persons and objects.

(3) Establish restricted areas to control access:

i) Define restricted areas. This may include cargo and ship stores transfer areas, passenger and crew embarkation areas, and locations where ships receive port services.

ii) Mark restricted areas.

iii) Develop restricted area access control policies. Physical means such as barriers and fences should be considered.

iv) Monitor restricted areas. This may include locking or securing access points, using surveillance equipment or personnel, using automatic intrusion detection devices, and issuing of maritime worker credentials.

v) Identify access points to the port, including waterways, rail lines, roadways, walkways, electronic information systems, and adjacent structures.

vi) Describe control measures for access points, including identification verification and frequency of application.

(4) Establish procedures for notifying vessels and facilities in the FMSC zone that MARSEC Levels 1 has been set.

(5) Designate areas where control measures shall be implemented.

(6) Deny access to anyone refusing to submit to security verification.

(7) Monitor the port, including during the hours of darkness and other times of poor or restricted visibility.

(8) Establish procedures and means of communicating any threatening acts.

(9) Supervise the handling of cargo and ship's stores. This may include cargo security procedures to prevent tampering, or inventory control procedures at access points.

(10) Offer to review physical security plans and procedures for facilities not regulated under 33 CFR 105, e.g., electrical transmission lines, communication transmitters, bridges, tunnels, mass transit bridges/tunnels, stadiums, aquariums, amusement parks, waterfront parks, marine events, nuclear power plants, and marinas.

(b) TAB E contains a consolidated table of recommended security measures for all MARSEC levels.

#### **4340 Operational Security (OPSEC) Measures**

(a) Operational Security is a process that protects information about capabilities and intentions by identifying, controlling, and protecting evidence of planning and execution of sensitive activities and operations.

(b) The information about our intentions, capabilities, or activities is known as "critical information." Since the compromise of this critical information may allow a terrorist to gain a significant advantage, its protection involves all maritime stakeholders. A concerted effort must be taken to ensure everyone is aware that the threat is real and active in all aspects of maritime security.

(c) Examples of critical information that should be protected from disclosure to unauthorized persons include:

- (1) Specific security measures being implemented (or not implemented)
- (2) Results of security assessments
- (3) Security vulnerabilities
- (4) Specific requirements listed in MARSEC Directives
- (5) Security Sensitive Information (SSI)

(d) Examples of practices that, if not properly managed/monitored, could lead to a compromise of critical information include:

- (1) Posting information to Web pages
- (2) Sending information via unsecured email/other electronic means
- (3) Posting information on bulletin boards
- (4) Telephone and radio communications
- (5) Conversations with persons without a "need to know"
- (6) Media interviews

(e) Operational Security Measures mitigate or control vulnerabilities and threats to, and usefulness of, information that our adversaries may develop. These measures can include procedural changes, suppression of indicators to deny critical information, deception, perception management, intelligence countermeasures, traditional (physical) security measures, or any other action that is likely to thwart our adversaries' purposes.

(f) The OPSEC Measures listed below are recommended at MARSEC Level 1. The FMSC may conduct occasional cursory spot checks to identify what measures are

being implemented and provide guidance or assistance as needed. Port stakeholders are encouraged to review these recommended measures and employ them as appropriate. **OPSEC Measures actually employed by any entity shall be designated as SSI and handled in accordance with Section 3500 of this Plan.**

Measure	Entity	Description
1	All	Minimize to the extent possible budgetary limitations related to security measures, systems, and forces.
2	All	Protect the security training status and records of personnel – make it difficult to learn who has completed what training and for what purpose they were trained.
3	All	Avoid descriptive or easily associated project names and exercise names, acronyms, and nicknames in conducting security business.
4	All	Periodically conduct surveillance of your own property and/or operation and identify signals/patterns/indicators that alert observers when you are about to conduct specific critical operations (e.g., pier lights always energized ½ hour before vessels arrive), and re-design so that these indicators are used for a variety of operations and periodically employed when no operation is on-going, thereby eliminating their value as true indicators for adversary surveillance.
5	All	Review web sites and public calendars that would indicate locations/schedules/activities of executives and critical personnel and remove this information.

#### **4400 MARSEC Level 2**

##### **4410 Roles, Resources, Authorities, and Responsibilities**

- (a) Generally the same as established in section 4310, however many agencies will have an increased law enforcement presence in place.
- (b) Tier 2 and/or 3 response and enforcement agencies (listed in Section 3200 of each FMSC Annex) may be activated and deployed.
- (c) The FMSC will consider implementing the Incident Command System (ICS) to manage port activities.

##### **4420 Standard Security Procedures for MARSEC Level 2**

- (a) Continue and enhance the actions taken under MARSEC 1. Each FMSC will review and implement security procedures as necessary given the current threat to detect, deter, disrupt, and respond to attacks against the MTS, its operations, and port infrastructure. Vessels and facilities required to have security plans under 33 CFR Parts 104 and 105 shall follow the additional required security procedures in their approved plan.
- (b) The FMSC will review current and upcoming Marine Event Permits and may require additional security measures or revoke the permit. See Section 4800 for additional information.
- (c) Each FMSC Annex will detail specific security procedures for their area. General measures to be implemented may include:
  - (1) Increase law enforcement presence in the port.

- (2) Increase coordination with the intelligence community.
- (3) Increase port monitoring activities, which may include overflights, waterside and landside patrols.
- (4) Increase communications and coordination with the AMS Committee and other port stakeholders.
- (5) Conduct spot checks of vessel and facility compliance with MARSEC measures.

#### **4430 Physical Security Measures**

(a) Vessels and facilities required to have security plans under 33 CFR Parts 104 and 105 shall implement the security measures outlined in their approved plan. All port entities not covered under Parts 104 and 105 are subject to this plan. Such entities should (and may be required to by a Captain of the Port Order) implement the following recommended security measures (as applicable):

- (1) Enhance security procedures identified for MARSEC Level 1.
- (2) Review security roles and responsibilities.
- (3) Control access to restricted areas to allow only authorized personnel.
- (4) Include mechanisms to ensure that regulated vessels and facilities:
  - i) Increase the frequency and detail of monitoring of restricted areas.
  - ii) Limit (or further limit) the number of access points, e.g., implement the use of physical means, such as barriers, fencing and personnel.
  - iii) Increase control of access points, e.g., assigning additional security personnel.
  - iv) Increase detail and frequency of monitoring, including inspection of individuals, personal effects, and vehicles.
  - v) Increase frequency of supervised handling of cargo and ship's stores.
- (5) Give consideration to requiring additional security measures for facilities not regulated under 33 CFR 105, e.g., electrical transmission lines, communication transmitters, bridges, tunnels, mass transit bridges/tunnels, stadiums, aquariums, amusement parks, waterfront parks, marine events, nuclear power plants, and marinas.

#### **4440 MARSEC 2 Verification and OPSEC Measures**

(a) The FMSC will verify the implementation of MARSEC Level 2 Physical Security measures and give consideration to requiring additional security measures. Within four hours of receiving reports of MARSEC 2 attainment, the FMSC will begin checks of measures employed by vessels, facilities, and other port entities covered under 33 CFR Subchapter H and immediately advise the owner/operator of any discrepancies. The FMSC should prioritize verification based on the current threats and risks.

(b) The OPSEC Measures listed below are recommended at MARSEC Level 2. The FMSC may conduct cursory spot checks within four hours of setting MARSEC 2 in

the port (or within four hours of receiving reports of MARSEC 2 attainment for vessels and facilities under 33 CFR Subchapter H) to identify what OPSEC measures are being implemented and provide guidance or assistance as needed. Port stakeholders are encouraged to review these recommended measures and employ them as appropriate. **All OPSEC Measures actually employed by any entity shall be designated as SSI and handled in accordance with Section 3500 of this Plan.**

Measure	Entity	Description
6	All	Continue MARSEC 1 OPSEC Measures.
7	All	Schedule operations and activities simultaneously so they mask each other and confuse observers as to what is happening and how the operations are related (if at all).
8	All	Disrupt anyone who might be monitoring your operations by occasionally rotating your communications procedures (from radio to cell phone to land-line) etc.
9	All	Gradually change your activity levels to meet MARSEC TWO requirements so the change is less apparent (while still meeting implementation time limits); gradually slow your activity levels after an "operational pause" so observers will not readily understand when the operational pause has ceased.
10	Commercial	Without disrupting operations, time activities to occur during periods of least security vulnerability.
11	All	To the extent possible, change the critical personnel reporting times and operational cycles in order to maximize adversary confusion. Vary the times and routes by which all executives and critical personnel report to work.
12	All	Minimize the use of e-mail and web pages to confer information about operational schedules, vessel arrival and departure times, and so on. Password protect fee-for-service web pages with vessel arrival and operational information on them.

### **4500 MARSEC Level 3**

#### **4510 Roles, Resources, Authorities, and Responsibilities**

- (a) Generally the same as established in section 4310, however many agencies will have an increased law enforcement presence in place.
- (b) Tier 2 and/or 3 response and enforcement agencies (listed in Section 3200 of each FMSC Annex) will likely be activated and deployed.
- (c) The FMSC will implement the Incident Command System (ICS) to manage port activities and establish Unified Command (UC) with appropriate authorities.

#### **4520 Standard Security Procedures for MARSEC Level 3**

- (a) Continue and enhance the actions taken under MARSEC 1 and 2. Each FMSC will review and implement security procedures as necessary given the current threat to detect, deter, disrupt, and respond to attacks against the MTS, its operations, and port infrastructure. Vessels and facilities required to have security plans under 33 CFR Parts 104 and 105 shall follow the additional required security procedures in their approved plan.
- (b) The FMSC will review current and upcoming Marine Event Permits and may require additional security measures or revoke the permit. See Section 4800 for additional information.

(c) Each FMSC Annex will detail specific security procedures for their area. General measures to be implemented may include:

- (1) Maximize law enforcement presence in the port, focusing on high risk assets or areas.
- (2) Intensify coordination with the intelligence community.
- (3) Increase port monitoring activities, which may include overflights, waterside and landside patrols.
- (4) Enhance communications and coordination with the AMS Committee and other port stakeholders.
- (5) Consider mobilizing Tier 2 and 3 response resources as detailed in Section 3200.

#### **4530 Physical Security Measures**

(a) Vessels and facilities required to have security plans under 33 CFR Parts 104 and 105 shall implement the security measures outlined in their approved plan. All port entities not covered under Parts 104 and 105 are subject to this plan. Such entities should (and may be required to by a Captain of the Port Order) implement the following recommended security measures (as applicable):

- (1) Continue and enhance security procedures required at MARSEC 1 and 2.
- (2) Identify and employ mechanisms to ensure that regulated vessels and facilities:
  - i) Monitor restricted areas to protect against an imminent security incident, e.g., secure all access points, prohibit storage of vehicles, cargo and ship's stores, and maintain continuous patrols.
  - ii) Control access, e.g., enhance the security presence at closed access points, provide escorts, and take measures, where practicable, to secure choke points and locations that can be used to observe facility or vessel operations.
  - iii) Protect against an imminent security incident, e.g., inspect all persons, personal effects and vehicles.
  - iv) Consider requiring additional security measures for facilities not regulated under 33 CFR 105, e.g., electrical transmission lines, communication transmitters, bridges, tunnels, mass transit bridges/tunnels, stadiums, aquariums, amusement parks, waterfront parks, marine events, nuclear power plants, and marinas.

(b) The FMSC will consider taking waterways management measures, which may include Safety/Security Zones, Regulated Navigation Areas, and waterway restrictions or closures.

(c) The FMSC may impose operational controls or restrictions on vessels and facilities.

(d) In the event of a significant security threat or breach, the FMSC in coordination with other federal, state or local authorities may order an evacuation within the port. The following minimum actions will be taken:

- (1) Transmit a Broadcast Notice to Mariners to alert and direct vessels.
- (2) Publish a Marine Safety Information Bulletin detailing evacuation procedures.
- (3) Establish security zone(s) and boundaries to control the potential crime scene while ensuring orderly evacuation of persons.
- (4) Ensure adequate enforcement of security zone(s).
- (5) Patrol and monitor affected area if possible.

#### **4540 MARSEC 3 Verification and OPSEC Measures**

(a) The FMSC will verify the implementation of MARSEC Level 3 measures and give consideration to requiring additional security measures. Within one hour of receiving reports of MARSEC 3 attainment, the FMSC will begin checks of measures employed by vessels, facilities, and other port entities covered under 33 CFR Subchapter H and immediately advise the owner/operator of any discrepancies. The FMSC should prioritize verification based on the current threats and risks.

(b) The attainment of OPSEC measures for MARSEC Level 3 will be verified by initial cursory spot-checks beginning within one hour of MARSEC Level 3 attainment. Regulated vessels and facilities, and vessels and facilities not regulated under parts 104, 105, and 106 will be checked. Observations for improvements will be relayed to the FMSC for further dissemination to parties responsible for corrective action via CSOs, FSOs, and VSOs. The WRAMS Committee and FMSC subcommittees may be engaged to assist in this effort.

(c) The OPSEC Measures listed below are recommended at MARSEC Level 3. The FMSC may conduct cursory spot checks within one hour of setting MARSEC 3 in the port (or within one hour of receiving reports of MARSEC 3 attainment for vessels and facilities under 33 CFR Subchapter H) to identify what OPSEC measures are being implemented and provide guidance or assistance as needed. Port stakeholders are encouraged to review these recommended measures and employ them as appropriate. **All OPSEC Measures actually employed by any entity shall be designated as SSI and handled in accordance with Section 3500 of this Plan.**

<b>Measure</b>	<b>Entity</b>	<b>Description</b>
13	All	Continue MARSEC 1 and 2 OPSEC Measures.
14	All	To the extent possible, change shift reporting times and operational cycles in order to maximize adversary confusion. Vary the times and routes by which all employees report to work, and consider staggered arrival times within one shift.
15	Marine Pilots; Tug Operators; Vessel Owners, Agents, and Operators; Facility Operators	Maintain absolute minimum advance notification (outside of government requirements and necessary docking arrangements) of exact arrival times, vessel names, and cargoes of vessels arriving in or departing the port. Keep notifications to ship chandlers, labor, etc., generic (rather than give away precise times, give a time-frame of 2 hours, etc.).

**4600 Public Access Facility**

(a) A facility that receives vessels certificated to carry 150 or more passengers is normally required to submit a Facility Security Plan and comply with all provisions of 33 CFR Part 105. However, such facilities that meet the definition of a Public Access Facility (PAF) may be exempted from certain requirements under that regulation.

(b) A Public Access Facility (PAF) is an area, designated by the FMSC, with public access that is primarily used for recreation or entertainment purposes, and which primary purpose does not include receiving or servicing vessels regulated under 33 CFR 104. This may include a public pier, wharf, dock, waterside restaurant or marina that contains no or minimal infrastructure, such as only bollards, cleats, or ticket booths, and occasionally receives vessels certificated to carry 150 or more passengers.

(1) A facility with permanent infrastructure such as boarding ramps, passenger receiving areas or staging/mooring barges will not normally be designated as a Public Access Facility and may be subject to the requirements under 33 CFR Part 105.

(2) Each FMSC Annex to this plan will list designated Public Access Facilities in their zone and provide contact information for the owner/operator.

**4610 Designation of Public Access Facilities**

(a) An owner or operator of a facility may send a written request to the appropriate FMSC to be designated as a PAF. Tab F includes a sample PAF designation request letter. The FMSC may also initiate the designation process.

(b) The FMSC will conduct a review and evaluation of the PAF designation request. This evaluation will consider the results and impacts related to the AMS Assessment. An on-site evaluation may be necessary to verify PAF applicability and identify security requirements.

(c) Once PAF designation applicability has been determined, the FMSC will coordinate with the owner or operator of the facility to establish the conditions under which the designation will be granted. Tab F includes a checklist of the minimum required and potential additional security measures the FMSC may impose. To ensure consistency between FMSC zones, any additional security measures should normally be limited to those listed in the "Additional Requirements to Review for Applicability" column.

(d) After an evaluation of the facility has been conducted and security conditions have been established, the FMSC will issue a PAF Designation Letter. Tab F includes a sample letter. At a minimum the letter shall include a list of established security conditions that shall be implemented at the PAF at each MARSEC level. Security conditions shall be included as an enclosure to the letter and are considered SSI. The owner or operator of the PAF shall acknowledge and accept these conditions in writing.

(e) A copy of the designation letter and acknowledgement, including the PAFs 24-hour contact information for the Individual with Security Responsibilities, shall be kept on file with the appropriate FMSC Annex to this plan for as long as the designation is valid.

**4620 Vessel Responsibilities When Calling at a PAF**

(a) Any vessel subject to 33 CFR Part 104 that intends to use a designated PAF must detail in their Vessel Security Plan how the security requirements listed below will be met. While the vessel is responsible for implementing these measures, they may liaison with the owner/operator of the PAF to determine who will actually perform the required security activities.

**(b) MARSEC 1 Vessel Responsibilities**

(1) Provide a 24-hour advance notice to the FMSC prior to arriving at the PAF.

(2) The vessel owner, operator, VSO or CSO should contact the Individual with Security Responsibilities at the PAF prior to their first visit to determine security measures that will be in place at the PAF. The appropriate FMSC Annex includes a list of PAFs, their designated Individual with Security Responsibilities and FMSC conditions/requirements for the PAF.

i) A vessel that frequently interfaces with the same PAF should also contact the Individual with Security Responsibilities at the PAF whenever there is a significant change in vessel operations.

ii) If the vessel is unable to contact the PAF prior to arrival, the vessel will perform all security activities and notify the FMSC.

(3) Prior to using the PAF, a sweep of the waterfront area shall be conducted to detect any dangerous substances or devices. The vessel may not use the PAF until the sweep is complete and satisfactory.

(4) While the vessel is at the PAF, the shoreside area must be continually monitored, within visual range of the vessel. A minimum of two persons shall be assigned to monitoring, and must have direct communications capability with vessel personnel and local law enforcement. Monitoring personnel may have additional duties or monitor multiple vessels so long as their view is not obstructed and they remain in the shoreside area of the vessel(s).

(5) If passenger baggage or vessel stores will be staged shoreside, a restricted area must be designated and monitoring personnel assigned to ensure the baggage/stores are not tampered with.

**(c) MARSEC 2 Vessel Responsibilities (in addition to MARSEC 1)**

(1) The vessel owner, operator, VSO or CSO must contact the Individual with Security Responsibilities at the PAF and execute a Declaration of Security (DoS) prior to each visit to coordinate security measures that will be in place at the PAF.

i) A vessel that frequently interfaces with the same PAF may execute a continuing DoS for multiple visits with an effective period of not more than 30 days.

ii) If the vessel is unable to contact the PAF prior to arrival, the vessel will perform all security activities and notify the FMSC.

(2) Arrange for separation of parking areas from vessel and passenger areas.

- (3) Increase monitoring of shoreside, passenger and baggage/ships stores areas.
- (d) MARSEC 3 Vessel Responsibilities (in addition to MARSEC 1 and 2)
  - (1) The vessel owner, operator, VSO or CSO must contact the Individual with Security Responsibilities at the PAF and execute a Declaration of Security (DoS) prior to each visit to coordinate security measures that will be in place at the PAF.
    - i) If the vessel is unable to contact the PAF prior to arrival, the vessel will perform all security activities and notify the FMSC.

#### **4630 Compliance and Enforcement**

- (a) Submission of Request for Designation as a Public Access Facility:
  - (1) Facilities that have submitted or are operating under an approved FSP that wish to be considered for designation as a PAF must submit a request to the FMSC at least 60 days prior to the requested designation date.
  - (2) Facilities not in operation before December 31, 2003 that wish to be considered for designation as a PAF must submit a request for Designation as a Public Access Facility to the COTP no later than 60 days prior to beginning operations.
    - i) If the FMSC does not approve the request, the facility will be subject to all requirements of 33 CFR Part 105. This includes the requirement to submit a Facility Security Plan at least 60 days prior to beginning operations.
  - (3) If a facility has a change in ownership, the Individual with Security Responsibilities must submit updated contact information to the FMSC. The owner/operator of the PAF shall conduct a review of the PAF designation and conditions and notify the FMSC of any changes to the facility's operations that may affect security requirements. The new owner/operator or Individual with Security Responsibilities must sign an acknowledgement of the PAF Designation letter and conditions.
- (b) After receiving the request, the FMSC will either:
  - (1) Approve it with conditions via PAF Designation letter,
  - (2) Request additional information to make a determination, or
  - (3) Disapprove it, with a letter restating the requirements under 33 CFR Part 105 (or a letter stating the facility does not meet the applicability requirements of 33 CFR Part 105).
- (c) The PAF designation and FMSC conditions will be evaluated annually to ensure they remain appropriate. Any changes to the operations or description of the facility must be immediately reported to the FMSC.
- (d) The PAF must operate under the conditions of the designation letter whenever an MTSA-regulated passenger vessel is at the facility. The Individual with Security Responsibility for the PAF, or the VSO for a visiting vessel, must notify the FMSC whenever the PAF is out of compliance. There are three anticipated types of non-compliance:

- (1) Incorrect contact information for the Individual with Security Responsibilities.
  - (2) The PAF will be temporarily out of compliance with the FMSC conditions.
  - (3) Permanent or frequent non-compliance.
- (e) Possible enforcement actions the FMSC may consider include:
- (1) Informal request for immediate correction/update for administrative discrepancies.
  - (2) FMSC letter requiring correction/update within a specified amount of time.
  - (3) COTP Order restricting or suspending operations with passenger vessels until the PAF is in compliance.
  - (4) Initiate civil penalty action.
  - (5) Revoke the designation as a PAF, requiring full compliance with 33 CFR Part 105, and consider issuing a COTP Order with conditions under which the facility may be allowed to operate until the FSP is approved.
- (f) The FMSC may withdraw a facility's designation as a PAF when the FMSC determines it is necessary. When a designation has been withdrawn from a facility that receives vessels regulated under 33 CFR Part 104, the facility will be required to comply with the requirements of 33 CFR Part 105.

#### **4640 Vessels Calling at a Non-MTSA Regulated Facility or Location**

- (a) Any vessel subject to 33 CFR Part 104 that intends to embark or disembark passengers at any facility other than one operating under an approved Facility Security Plan or a designated Public Access Facility (this definition of "facility" includes any location where temporary structures or augmentations, such as the addition of a mooring barge, boat ramp etc. are made to an existing pier or ramp) must request approval from the cognizant Coast Guard District Commander, via the FMSC, at least 60 days in advance. This waiver may be approved for a one-time visit only. Any subsequent requests for a waiver at the same facility must be forwarded to Commandant (G-MP). If approved, the vessel will be responsible for implementing all shoreside and vessel security measures.
- (b) Any vessel subject to 33 CFR Part 104 that intends to embark or disembark passengers at any location that is not a facility (i.e. there is no structure, such as along a river bank) must notify and receive permission from the FMSC at least 24 hours in advance. If approved, the vessel will be responsible for implementing all shoreside and vessel security measures.

#### **4700 Maritime Worker Credentials**

- (a) The USCG has published guidelines in the Federal Register (vol. 67, no.152, pgs. 51082-51083), which describe the proposed requirements for maritime identification credentials. When finalized, every person (including foreign seafarers) entering a U.S. port facility, or embarking or debarking a vessel will be required to carry, at a minimum,

a laminated (or otherwise secured from tampering) identification card that displays the holder's full name and current photograph and the name of issuing authority or company.

(b) Until these requirements are finalized, government-issued picture identification is the most valid type of identification when required for access to a facility or vessel. These may include, but are not limited to, drivers' licenses, military identification cards, Merchant Mariner Documents (MMD), etc. Law Enforcement credentials will also be considered a valid type of identification.

#### **4800 Marine Events**

(a) Organizers of certain marine-related events are required under 33 CFR Part 100 to submit a request for a Marine Event Permit to the Coast Guard. This procedure was initially implemented to ensure safety issues were addressed. With the implementation of MTSA, the FMSC must also consider security related issues while reviewing the application. The following minimum security concerns must be addressed:

- (1) Communications between the event organizer and participants.
- (2) Communications between the event organizer and security / law enforcement assets (shoreside and waterside).
- (3) Continuous monitoring for suspicious activities (shoreside and waterside).
- (4) Crowd control, which may include entry screening in case of a potential security concern.
- (5) Evacuation plan, which may include departure screening to detect possible perpetrators.

(b) When MARSEC Level 2 or 3 is set, the FMSC shall review current and upcoming Marine Event Permits and may require additional security measures or revoke the permit. Additional requirements will be issued under a Captain of the Port Order and may include (but are not limited to):

- (1) Additional waterside monitoring and/or crowd control.
- (2) Restrictions on the number of participant and spectator vessels.
- (3) Additional shoreside monitoring.

(c) Organizers of events adjacent to waterways that do not meet the requirements of 33 CFR Part 100 but anticipate more than 500 attendees shall ensure appropriate permits are granted. Permit approval by federal, state or local authorities should be coordinated with the FMSC and local AMS Committee. The following security concerns should be addressed:

- (1) Communications between the event organizer and participants.
- (2) Communications between the event organizer and security / law enforcement assets (shoreside and waterside).
- (3) Continuous monitoring for suspicious activities (shoreside and waterside).
- (4) Crowd control, which may include entry screening in case of a potential security concern.

- (5) Evacuation plan, which may include departure screening to detect possible perpetrators.
- (6) Additional actions to be taken when MARSEC Level 2 or 3 is set.

## **5000 PREPAREDNESS FOR RESPONSE**

### **5100 Introduction**

(a) Preparedness for response in the context of the AMS Plan is primarily designed to provide post-incident response and mitigation linkages. This section provides guidance to each FMSC in collecting the information necessary to identify the following:

- (1) Who will respond to the specific security threats or incidents.
- (2) What resources responders will bring with them.
- (3) The incident command structure.
- (4) The communications required to mitigate the impact of a TSI.

### **5110 Procedures for Responding to Suspicious Activity**

(a) General procedures for response are:

- (1) The affected entity or person observing the suspicious activity notifies their internal security staff (if applicable), local law enforcement, the FMSC and the National Response Center. Tab C provides forms for collecting and reporting information.
- (2) Internal security staff and/or local LE investigate the activity and take necessary actions to maintain security at the site. Section 3700 of each FMSC Annex lists response agencies and expected timeframes for dispatch (if available).
- (3) The FMSC will communicate with the initial responders to determine the scope and severity of the activity and coordinate additional response or investigative assets if needed.
- (4) The FMSC will share information with the AMS Committee and other port stakeholders as appropriate to increase security. This information may be designated as SSI and must be reviewed to prevent release of proprietary or law enforcement sensitive information.

### **5120 Procedures for Responding to Breaches of Security**

(a) Pursuant to 33 CFR 101.105, a “Breach of Security” is defined as “an incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded or violated.”

(b) The local AMS Committee shall consider geographic capabilities of Federal, State, and local law enforcement entities (listed in Section 3200) and consequence mitigation resources in determining which entities will respond to breaches of security at high consequence targets.

(c) General procedures for response are:

- (1) The affected entity notifies their internal security staff, local law enforcement, the FMSC and the National Response Center. Tab C provides forms for collecting and reporting information.
- (2) Internal security staff and/or local LE investigate the activity and take necessary actions to maintain/restore security at the site. Section 3700 of each FMSC Annex lists response agencies and expected timeframes for dispatch (if available).
- (3) The FMSC will communicate with the initial responders to determine the scope and severity of the breach and coordinate additional response or investigative assets if needed.
- (4) The FMSC will coordinate response actions with all involved parties.
- (5) The FMSC will consider requiring additional security measures for potentially affected entities.
- (6) The FMSC will share information with the AMS Committee and other port stakeholders as appropriate to increase security. This information may be designated as SSI and must be reviewed to prevent release of proprietary or law enforcement sensitive information.

## **5200 Transportation Security Incident (TSI)**

### **5210 Procedures for Notification**

A TSI will first be reported to the appropriate emergency services to ensure human health and safety measures are taken. Secondary notifications will be made to the FMSC or their representative, then to the NRC. Refer to Tab C for a sample Quick Response Card for reporting a TSI.

### **5220 Incident Command Activation**

- (a) First responders may establish an incident command structure on scene during the initial response to a TSI.
- (b) As the response develops the FMSC will assess jurisdiction and determine the Lead Federal Agency (LFA). In consultation with partner agencies, the LFA will determine whether there is a need to establish an ICS/UC, what its structure will be and establish a command post or operations center.
- (c) If the Coast Guard is the LFA, the National Incident Management System (NIMS) Incident Command System will be established per current policy. Any previously established ICS shall be integrated into the UC. Section 5310 includes example ICS Structures for responding to potential TSIs.
- (d) For significant incidents, DHS may activate the Federal Response Plan (FRP) / National Response Plan (NRP) and assume or designate the role of LFA and supporting agencies.
- (e) During an actual terrorism event, the FBI may assume the role of LFA and implement the Interagency Domestic Terrorism Concept of Operations Plan (CONPLAN).

**5230 Threats that Do Not Rise to the Level of a TSI**

There will be threats, causes for concern, and violations of existing security plans that are worth investigation, but do not rise to the level of a TSI. This could be due to simple miscommunications, lost credentials, an innocent person unaware of entry restrictions or perimeters, etc. In most of these cases, simple resolution of the problem or referral to appropriate authorities is the only action needed. Notification shall also be made to the NRC. Incidents that reveal serious discrepancies or weaknesses within required plans should be reported to the FMSC.

**5300 Most Probable Transportation Security Incident**

- (a) Because each port area has unique characteristics, different types of TSIs are likely to occur more frequently in one port area than another. FMSCs should use the results of the AMS Assessment to identify the three types of TSIs most likely to occur within their zones.
- (b) Since it is impossible to plan for every scenario, FMSCs and AMS Committees are directed to plan for a minimum of three scenarios that require exercise of command and control procedures, communications, and the initial response to be taken by port agencies. These plans will be viewed as unofficial Memorandums of Agreement (MOAs) within the port to ensure key players understand what activities each agency will take, and what resources each will bring for the given scenario.
- (c) Scenarios should focus on threats and vulnerabilities applicable to that port, such as threats to the common infrastructure, general port threats, and those threats that affect other regulated vessels or facilities.
- (d) The scenarios listed below are considered the most probable TSIs for the Western Rivers region:

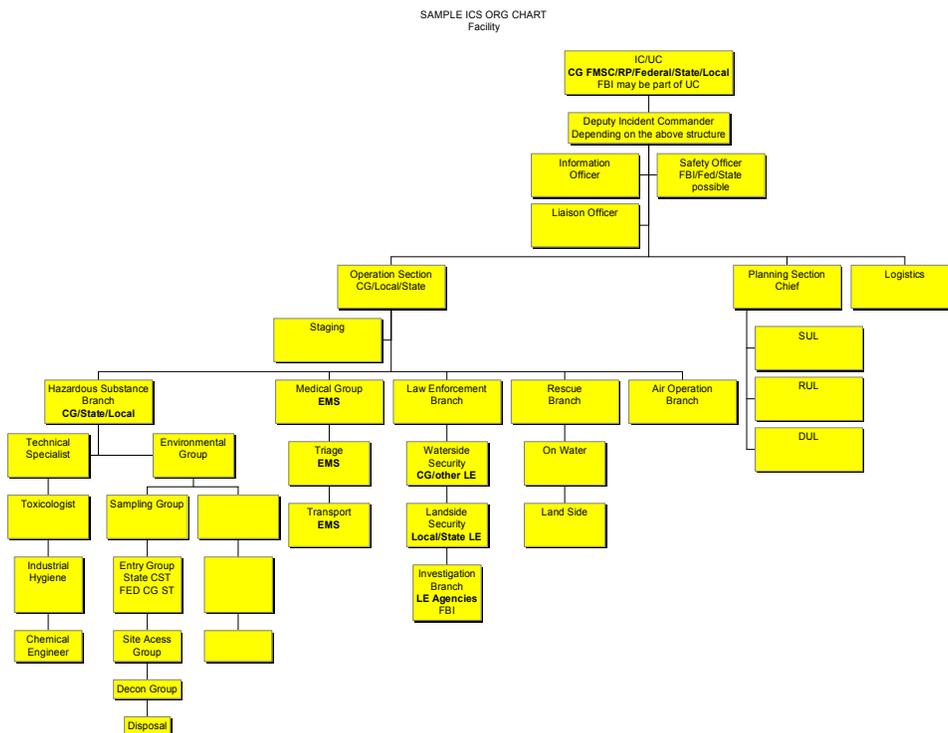
Target	Method	Primary Consequence
High Density Population Area	Release or detonation of Certain Dangerous Cargoes (CDC)	Mass Casualties Major Environmental Threat
Marine Event	Detonation of a fireworks barge or explosive-laden recreational vessel	Mass Evacuation
Passenger Vessel	Hijacking/intentional collision or WMD attack	Mass Casualties
Facility (regulated or non-regulated)	Intrusion and intentional damage or destruction	Major Environmental Threat Mass Casualties
Lock, Dam or Major Bridge	Detonation of explosive device or CDC barge, or ramming by commercial vessel	Major Economic Disruption Mass Casualties

(e) Since the AMS Plan is not a response plan, but an awareness, preparedness and prevention plan, scenario development considered possible roles, responsibilities, and resources very broadly and was limited to determining who will respond, what their roles will be, and what resources they can provide.

**5310 Identify Command Structure with Assigned Roles (ICS Flowchart)**

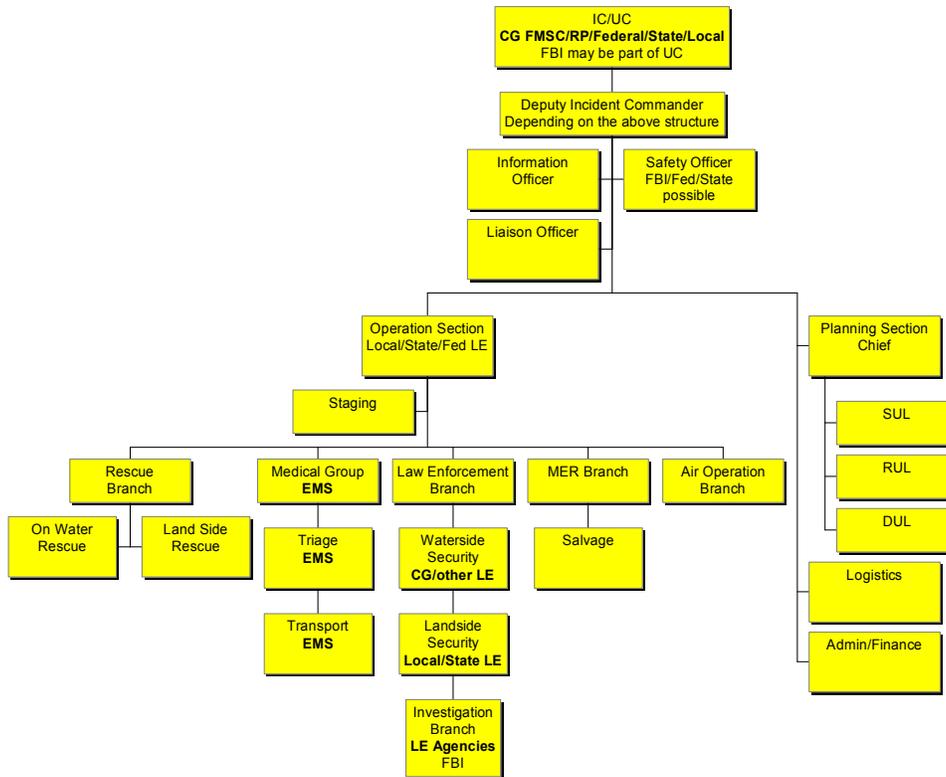
(a) Model ICS Structures for the most probable TSIs listed above are provided below.

**High Density Population Area or Facility or Lock/Dam/Bridge:**



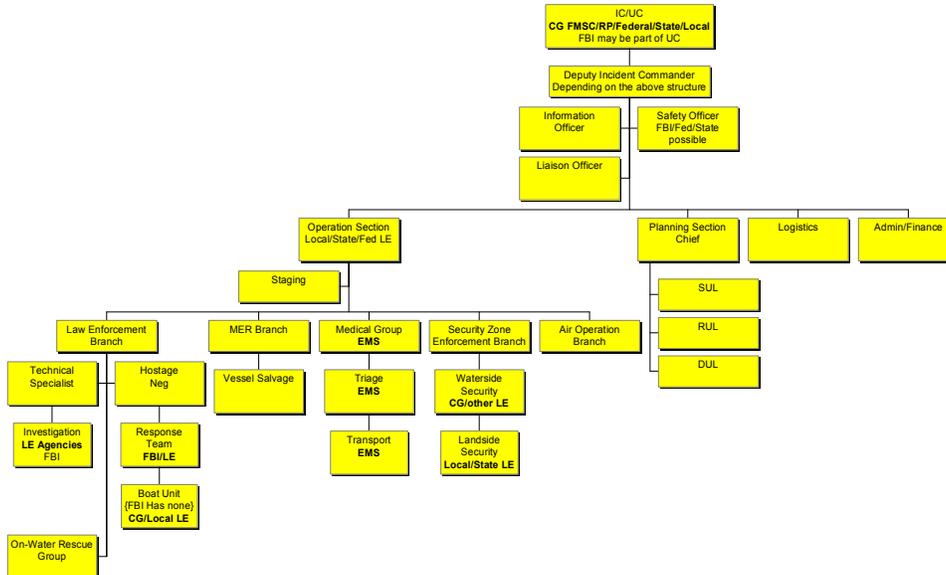
**Marine Event:**

SAMPLE ICS ORG CHART  
Marine Event, explosive adjacent to target



**Passenger Vessel:**

SAMPLE ICS ORG CHART  
Taking over vessel/hostages/ramming other vessels



**5320 Procedure for Responding to a TSI**

(a) Responding agencies will participate in an ICS/UC to coordinate response actions and use of resources. Section 3700 of each FMSC Annex lists response agencies and expected timeframes for dispatch (if available).

(b) General procedures for response are:

(1) The affected entity notifies their internal security staff, local law enforcement, the FMSC and the National Response Center. Tab C provides forms for collecting and reporting information.

(2) Internal security staff and/or local LE investigate the activity and take necessary actions to maintain/restore security at the site.

(3) Other first responders, such as fire or Emergency Medical Services (EMS), will mitigate fire, hazardous materials and other safety concerns in coordination with LE to preserve the potential crime scene and facilitate investigation.

(4) The FMSC will implement ICS/UC and communicate with the initial responders to determine the scope and severity of the incident and coordinate additional response or investigative assets if needed.

(5) The FMSC will coordinate response actions with all involved parties.

(6) The FMSC will consider requiring additional security measures for potentially affected entities.

(7) The FMSC will share information with the AMS Committee and other port stakeholders as appropriate to increase security. This information may be designated as SSI and must be reviewed to prevent release of proprietary or law enforcement sensitive information.

**5330 Linkage with Applicable Federal, State, Port & Local Plans**

(a) The AMS Plan contains information that pertains to prevention of security incidents, such as procedures for communication and coordination to reduce the risk of, or vulnerability to terrorist acts. To be effective when terrorist acts result in security incidents, the procedures detailed in the AMS Plan must be coordinated with incident response plans. Therefore the FMSC shall ensure coordination with relevant crisis management plans for contemplated security incidents, and that such plans are referenced in the AMS Plan.

(b) In the event of a terrorist attack, the following plans should be reviewed and considered by the USCG during the crisis management phase: Applicable response plans include:

(1) National Oil and Hazardous Material Spill Response Plan (NCP).

(2) The Federal Response Plan (FRP) / National Response Plan (NRP).

(3) Area Contingency Plans (ACP).

(4) Maritime Counter-Terrorism Contingency Plan.

(5) United States Government Interagency Domestic Terrorism Concept of Operations Plan (CONPLAN).

(6) USCG 9700 series Plans and Appendices.

(7) State and Local emergency response plans (addressed in FMSC Annexes).

(c) Section 4530 lists procedures to be taken for an evacuation of the port.

#### **5400 Maritime Security Exercise Requirements**

(a) The recommended methodology for building an effective exercise program is the Talk, Crawl, Walk and Run progressive training system. The four stages of the system are:

(1) Talk: This is the stage wherein AMS Committees meet to discuss various scenarios and review duties and responsibilities for each of the critical decision makers. This affords the opportunity to eliminate unfamiliar terminology and clarify communications procedures. This may include a Tabletop Exercise.

(2) Crawl: At this stage, a telephonic alert (Notification Exercise) to test the emergency contact system may be used. Other primary and alternate methods of communications should also be tested. It is recommended that this phase be tested at different times to discover any communication problems that may occur at any given time. To find the most reliable method, several methods of contact should be attempted and then incorporated into the primary method.

(3) Walk: This stage will include an announced exercise that tests the ability of the crisis operations committee to form and perform at their initial stages of crisis response planning. Effective area analysis will be performed to find out when and where traffic and other routine activities may interfere with the crisis response. This is commonly referred to as a Functional Exercise.

(4) Run: This is a Full Scale Exercise (also known as a Field Exercise) that will involve multi-agency and multi-echelon crisis response elements that range from first responders through third responders. This exercise will be advertised so as to avoid public alarm. It is recommended that at least one type of scenario be staged and executed followed by an After Action Review. If feasible, multiple scenarios of different types should be staged and executed while all participants are gathered and available to ensure maximum benefit of the use of resources, since many key players must sacrifice substantial amounts of time and resources to participate in exercises.

(b) In order for the exercise to be successful, it must be as realistic as possible. The community will be involved to the fullest extent possible.

#### **5410 Purpose of Exercise Program**

(a) The AMS Plan will be tested periodically for currency and efficiency, and to evaluate risk mitigation strategies incorporated into the AMS Plan. Exercise design will be based on threat information and encompass procedures for setting MARSEC Levels. An exercise may consist of any of the types listed in Section 5400, or a combination thereof.

(b) The exercise program will focus on risk reduction methodologies, and be designed to determine the methodologies' validity and serve as a measurement tool for evaluating and improving the risk reduction methods identified in the Plan. Results are expected to assist in updating and improving AMS Committee coordination, close gaps within the AMS Plan, and improve the overall security of the FMSC zone.

#### **5420 Goals of the AMS Plan Exercise Program**

(a) The following goals of the Exercise Program should shape the development of exercise scenarios:

- (1) Identification of performance-based components of the mitigation strategy.
- (2) Gauging the effectiveness of enhanced security measures employed at port infrastructure within the area.
- (3) Creating a pool of lessons learned.
- (4) Establishing interaction protocols with other Federal, State and local law enforcement agencies likely to be involved in the overall protection of MTS.
- (5) Updating the AMS Plan.

#### **5430 Exercise Cycle**

Each FMSC shall coordinate with the AMS Committee(s) in their zone to conduct or participate in an exercise at least once per calendar year, with no more than 18 months between exercises, to test the effectiveness of the AMS Plan. The WR AMS Committee will provide exercise program guidance to the FMSCs as appropriate.

The exercise and planning cycles will be closely linked for all exercise held within the Western Rivers Region. Specific sections of the WRAMS Plan and the FMSCs' local AMS plans will be selected for evaluation during drills and exercises. The lessons learned from such drills and exercises will be incorporated into updates of the WRAMS Plan and local AMS plans during their next planned update cycles.

#### **5440 Scheduling And Design**

(a) The FMSC shall follow existing Coast Guard guidance for scheduling and designing AMS exercises. The following will be included in designing the exercise program:

- (1) Objectives: Develop exercise goals.
- (2) Concept Development: How will the objectives be attained?
- (3) Scenario and Strategy Selection: Determine the correct strategy and scenario selection to meet exercise objectives.
- (4) Conduct of Exercise: Define how the exercise will meet design objectives and detail scope.
- (5) Control and Evaluation: Detail evaluation and control protocols.
- (6) Data Collection: How will the data be fused?

(7) After-Action Report: The report will include all aspects of the evaluation process and detail corrective action.

(8) Corrective-Action Plan: How will the corrective action be undertaken?

**5450 Consideration of Equivalent Response**

(a) When the AMS Plan is implemented in response to an actual threat, the AMS Committee may request credit toward meeting any relevant portion of a Plan exercise requirement. The reviewing District Commander, and the Area Commander giving the credit, will ensure that useful information regarding strategy validation and process improvement is generated for the purpose of evaluating the effectiveness of the Plan strategies actually implemented.

(b) Credit may be requested for participation in other Federal, State, municipal, or private sector exercise programs. To receive credit, the exercise must implement AMS Plan strategies.

**5460 Record Keeping**

Exercise documentation must be retained by the FMSC for 2 years in accordance with existing Coast Guard exercise guidance. The local AMS Committee Secretary will ensure that all exercise documentation required to be marked as SSI is properly marked and protected from release to the general public.

**5470 Linkages Between Family of Plans within the Area**

(a) The WR AMS Plan is part of a “family of plans.” The “family of plans” concept requires that all security plans be considered in developing the overall security posture for the port. The AMS Plan works in conjunction with the security plans for vessels and facilities. To be effective, the procedures detailed within the AMS Plan must be coordinated with other security, incident response, crisis management and consequence management plans.

(b) The following linkages should be considered:

(1) Facility security plans required under 33 CFR Part 105.

(2) Vessel security plans required under 33 CFR Part 104.

(3) Passenger Vessel Security Plans.

(4) Area Maritime Security Plans Adjacent to the Western Rivers Region: The consolidated approach encompasses the nine WR FMSC zones and provides for coordination and consistency throughout the WR region. The WR AMS Plan will be a stand-alone document developed in a collective effort to address commonalities among the participating FMSC zones, and will also incorporate individual FMSC annexes to address unique assets and resources. The WR AMS Plan should not conflict with the security plans of other jurisdictions. The WR AMS Committee will work with other jurisdictions or agencies either directly or through USCG district or area staff elements to resolve any conflicts.

(5) Railroad Operation Security Plans.

(6) Other Federal, State and local plans.

## **6000 CRISIS MANAGEMENT AND RECOVERY**

### **6100 Introduction**

The United States' policy on responding to domestic incidents is outlined in Homeland Security Presidential Directive 5 (HSPD-5), Management of Domestic Incidents; and Homeland Security Presidential Directive 8, (HSPD-8), National Preparedness. HSPD-5 establishes a comprehensive national incident management system to enhance the ability of the United States to manage domestic incidents. HSPD-8 establishes policy to strengthen the preparedness of the United States to respond to threatened or actual domestic terrorist attacks, major disasters, and other emergencies by requiring a national domestic all-hazards preparedness goal, establishing mechanisms for improved delivery of Federal preparedness assistance to State and local governments, and outlining a plan to strengthen preparedness capabilities of Federal, State and local entities. The WRAMS Plan must coordinate with federal, state and local crisis management plans involving maritime infrastructure.

The general priorities of the maritime transportation system for protection and recovery are:

- (1) Major transportation routes needed for emergency services, including tunnels, bridges, and key waterways.
- (2) Main shipping channels critical for homeland security and homeland defense operations.
- (3) Port areas critical for military traffic or outloads.
- (4) Secondary bridges and tunnels.
- (5) Main shipping channels critical to commercial operations.
- (6) Secondary commercial waterways.
- (7) Public/recreational waterways.

Procedures for prioritizing and protecting port infrastructure are addressed in sections 4330, 4430, and 4530 of this plan. In addition, each annex in this plan separately addresses the priorities and provides protection and recovery strategies for the marine transportation system in each FMSC zone.

### **6200 Procedures to Maintain Infrastructure**

Section 9300 of each FMSC Annex includes a prioritized list of types/categories of port operations and infrastructure in their zone, and the number of each. This information was used by the AMS Committee to develop procedures for maintaining infrastructure integrity, which are identified in Sections 43xx, 44xx and 45xx of each FMSC Annex. This information is considered Sensitive Security Information and must be protected accordingly.

### **6300 Procedures for Recovery of MTS**

(a) Procedures for recovery of the MTS and reopening of the port(s) or affected waterways include:

- (1) Coordination with agencies and port stakeholders (normally establish ICS/UC).
  - (2) Safety of life and health / Search and rescue.
  - (3) Damage assessment (overflight is preferred).
  - (4) Channel survey.
  - (5) Debris removal.
  - (6) Restoration of essential Aids to Navigation.
  - (7) Resume commercial shipping and other port operations, with operational restrictions as needed.
- (b) General priorities for recovery are:
- (1) Restore major transportation routes needed for emergency services, including tunnels, bridges, and key waterways.
  - (2) Main shipping channels critical for homeland security and homeland defense operations.
  - (3) Port areas and channels critical for military traffic or outloads.
  - (4) Secondary bridges and tunnels.
  - (5) Main shipping channels critical to major commercial operations.
  - (6) Secondary commercial waterways.
  - (7) Public/recreational waterways.

## **7000 COMPLIANCE MEASURES**

The MTSA regulations rely on existing COTP authority if compliance measures need to be taken. Operational controls are normally exercised as a preventative measure when it is necessary to secure nonconforming vessels or facilities to adequately reduce or prevent risks of injury or damage to vessels or facilities. The control and compliance measures contained in 33 CFR 101.410 provide the FMSC with a large degree of flexibility to gain the compliance of both vessels and facilities operating with the zone.

### **7100 Control and Compliance Measures**

- (a) The FMSC may exercise authority pursuant to 33 CFR parts 6, 160 and 165, as appropriate, to rectify non-compliance with MTSA regulations. FMSC or their designees are the officers duly authorized to exercise control and compliance measures.
- (b) Control and compliance measures for vessels not in compliance with 33 CFR Subchapter H may include, but are not limited to, one or more of the following:
  - (1) Inspection of the vessel.
  - (2) Delay of the vessel.
  - (3) Detention of the vessel.
  - (4) Restriction of vessel operations.

- (5) Denial of port entry.
  - (6) Expulsion from port.
  - (7) Lesser administrative and corrective measures.
  - (8) Suspension or revocation of a security plan approved by the U.S., thereby making that vessel ineligible to operate in, on, or under waters subject to the jurisdiction of the U.S.
- (c) Control and compliance measures for facilities not in compliance with 33 CFR Subchapter H may include, but are not limited to, one or more of the following:
- (1) Restrictions on facility access.
  - (2) Conditions on facility operations.
  - (3) Suspension of facility operations.
  - (4) Lesser administrative and corrective measures.
  - (5) Suspension or revocation of security plan approval, thereby making the facility ineligible to operate in, on, under or adjacent to waters subject to the jurisdiction of the U.S.
- (d) Control and compliance measures may be imposed on a vessel that has recently called on a facility or at a port that does not maintain adequate security measures. These measures will be imposed to ensure that the vessel's security has not been compromised.

#### **7200 Enforcement**

The FMSC should work cooperatively with those in substantial compliance to help them achieve full compliance, use civil penalties for those who are not making satisfactory progress, terminate or suspend the operations of any owner or operator who has not attempted to comply, and pursue criminal action for egregious cases or willful noncompliance. The FMSC may impose control and compliance measures for vessels and facilities not in compliance such as amending or suspending the certificate of inspection or issuing a COTP order to cease MTSA-regulated operations until a vessel or facility is in compliance with an approved plan.

#### **7300 MARSEC Compliance**

- (a) Facility compliance with MARSEC Level/Directive requirements may be verified by:
- (1) FMSC visits.
  - (2) Facility report of compliance or noncompliance with various MARSEC levels.
  - (3) Spot check of certain facilities based on:
    - (4) Facility history
    - (5) Quality of previous implementation
    - (6) Risk level
    - (7) Regulatory inspections.
  - (8) During casualty response.

- (b) Vessel compliance may be verified by:
  - (1) Vessel boardings.
  - (2) Operator reports.
  - (3) Spot checks.
  - (4) Regulatory inspections.
  - (5) During casualty response.

## **8000 PLAN DOCUMENTATION AND MAINTENANCE**

### **8100 Initial Plan Review and Comment**

- (a) The WRAMSPC developed the regional portion of this plan and provided oversight/guidance for development of the FMSC Annexes. The WRAMSPC submitted the WR AMS Plan (including annexes for each FMSC zone) to the Commander, Eighth Coast Guard District. The appropriate sections of the Plan are designated SSI.
- (b) The Eighth District Commander will conduct the initial AMS Plan review. When conducting the initial review, the District Commander will review the AMS Plan for completeness and content and forward it to the Atlantic Area Commander who is the approving authority. Upon approval, Area will forward an electronic version of all approved AMS Plans to Commandant (G-MP).

### **8110 Procedures for Continuous Review and Update of the AMS Plan**

- (a) The AMS Plan is a living document that must be periodically updated to address the ever-changing terrorist threat landscape.
- (b) Annual Review. The update and review of the AMS Plan is an ongoing process. The WRAMSPC will review the regional portion of this plan at least annually for accuracy, feasibility, consistency and completeness. Each FMSC, in conjunction with local AMS Committees, will review their annex at least annually. Local AMS Committees are encouraged to establish Plan Review Work Groups that meet on a regular basis to facilitate this process.
- (c) The plan should also be reviewed after each activation, exercise, or drill, and when port conditions change. After each review, the plan will be updated to include any lessons learned from the activation exercise and drill, and to reflect changing port conditions.
- (d) Formal Review. The AMS Committee will conduct a detailed review every 5 years as required by the MTSA. This will require a review of the security assessment of the area covered by the Plan. This will allow for accounting of evolving infrastructure changes.
- (e) Portions of the AMS Plan must be updated immediately when certain critical items of information change, including:
  - (1) Emergency points of contact by name and number.
  - (2) Any changes that alter the communications or notification plan.

- (3) Any changes in jurisdictional or response capabilities.
- (4) Any major or minor construction changes that alter avenues of access to facilities.
- (f) Administrative and clerical updates to the plan (corporate name changes, personnel changes, etc) may be approved on an on-going and as-needed basis by the FMSC.
- (g) Updates of the AMS Plan will be submitted to the Coast Guard Eighth District and Atlantic Area Commanders for review and approval annually, or as substantive changes are made.

### **8120 Procedures for Continuous Review and Update of the AMS Assessment**

- (a) The AMS Assessment will also be reviewed and updated to incorporate changes in the port operations and infrastructure. Like the AMS Plan update and review, conducting routine area maritime security assessments is an on-going process. Accordingly, the assessment should be informally evaluated at least annually for adequacy, feasibility, consistency, completeness, and to identify gaps in security.
- (b) Additional review of the AMS Assessments should be conducted as vulnerabilities change among port infrastructure and facilities, or when assessment priorities/guidance changes.

## **9000 APPENDICES**

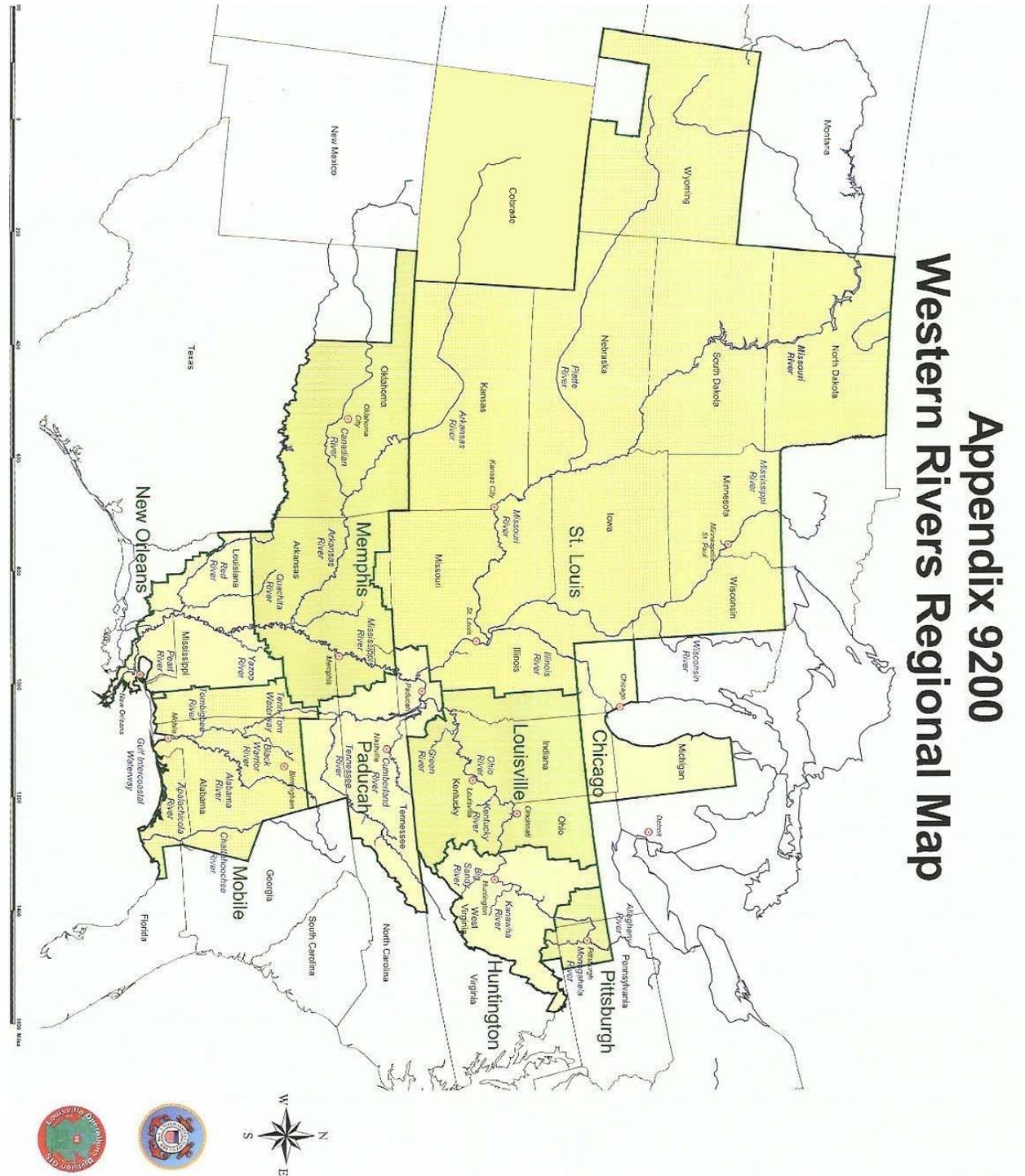
The AMS Plan contains some information that is intended to reach a broad array of maritime interests while other portions of the AMS Plan will be designated as SSI. Some information contained in the Plan is better suited in the form of an appendix due to the size or sensitive nature of the information. Depending on distribution, appendices may be omitted from copies of this plan due to being designated SSI.

### **9100 WR AMS Executive Steering Committee Members**

<b>Organization</b>	<b>Committee Member</b>	<b>Position</b>	<b>Telephone Numbers</b>	<b>Email</b>
Eighth Coast Guard District	Captain Frank Paskewich	Chairperson	O (504) 589-3647	<a href="mailto:fpaskewich@d8.uscg.mil">fpaskewich@d8.uscg.mil</a>
Eighth Coast Guard District	Harvey Dexter	Executive Secretary	O (504) 589-3043	<a href="mailto:hdexter@d8.uscg.mil">hdexter@d8.uscg.mil</a>
Transportation Security Administration	James Clarkson	Committee Member	O (571) 227-3554	<a href="mailto:james.Clarkson@dhs.gov">james.Clarkson@dhs.gov</a>
Maritime Administration	Robert Goodwin	Committee Member	O (314) 539-6783 C (812) 989-4768	<a href="mailto:robert.Goodwin@marad.dot.gov">robert.Goodwin@marad.dot.gov</a>
U.S. Army Corps of Engineers (Mississippi Valley Division)	Mark Faith	Committee Member	O (601) 631-7394	<a href="mailto:mark.faith@usace.army.mil">mark.faith@usace.army.mil</a>

U.S. Army Corps of Engineers (Great Lakes and Ohio River Ohio Division)	John Cheek	Committee Member	O (513) 684-6210	<a href="mailto:john.d.cheek@lrdor.usace.army.mil">john.d.cheek@lrdor.usace.army.mil</a>
NORTHCOM	TBD Pending Assignment	Committee Member		
TRANSCOM	Alan Colvin	Committee Member	O (618) 229-1460	<a href="mailto:alan.colvin@hq.transcom.mil">alan.colvin@hq.transcom.mil</a>
Towing Safety Advisory Committee	Mario Munoz	Committee Member	O (812) 288-0347 C (502) 552-3831	<a href="mailto:mario.Munoz@acbl.net">mario.Munoz@acbl.net</a>
Chemical Transportation Advisory Committee	TBD Pending Assignment	Committee Member		
American Waterways Operators	Lynn Muench	Committee Member	O (314) 621-2929 C (314) 308-0378	<a href="mailto:Awo-midcontinent@msn.com">Awo-midcontinent@msn.com</a>
Passenger Vessel Association	Gary Frommelt	Committee Member	O (636) 940-4472 C (314) 308-4827	<a href="mailto:gfrommelt@msn.com">gfrommelt@msn.com</a>
Barge Fleeting Representative	George P. Foster	Committee Member	O (314) 894-3805	<a href="mailto:georgefoster@jbmarineco.com">georgefoster@jbmarineco.com</a>
American Gaming Association	Jon Glantz	Committee Member	O (636) 458-9363 C (636) 346-7722	<a href="mailto:jsglantz@earthlink.net">jsglantz@earthlink.net</a> ; <a href="mailto:jsglantz@yahoo.com">jsglantz@yahoo.com</a> ; <a href="mailto:jonglantz@boydgaming.com">jonglantz@boydgaming.com</a>
Inland Rivers, Ports and Terminals	Deirdre McGowan	Committee Member	O (601) 352-4778 C (601) 214-1649	<a href="mailto:admin@irpt.net">admin@irpt.net</a>
Customs and Border Protection	John Porter	Committee Member	O (314) 428-2662 ext. 201	<a href="mailto:John.s.porter@dhs.gov">John.s.porter@dhs.gov</a>

9200 Western Rivers Regional Map



**9300 Port Operations and Infrastructure**

Each FMSC Annex will include information on critical port operations and infrastructure. Due to the nature of this information it may be designated SSI, and maintained separately from the AMS Plan in accordance with 49 CFR part 1520.

**9400 Risk-Based Scenarios**

(a) The following scenarios were used in the development of the Coast Guard Port Security Risk Assessment Tool (PSRAT):

- (1) External attack by moving explosives adjacent to the target.
- (2) External attack by weapons launched from a distance.
- (3) Intrude/take control and create Chemical, Biological, Radiological, Nuclear and Explosive (CBRN&E) or pollution incident without destroying target.
- (4) Intrude/take control and damage/destroy the target with explosives.
- (5) Intrude/take control and damage/destroy the target through malicious operations/acts.
- (6) External attack by ramming vessel/boat into a target.
- (7) Intrude/take control and take hostages/kill people.

**9500 Dangerous Cargos for Security Planning**

(a) Refer to 33 CFR Parts 126, 127 and 154 for a list of all dangerous cargoes regulated under 33 CFR Part 105 (Facility Security).

(b) Certain Dangerous Cargoes (CDC) are defined in 33 CFR 160.204. CDCs most commonly carried on the Western Rivers are:

Acetone cyanohydrin	Acetylaldehyde
Allyl alcohol	Anhydrous Ammonia
Butdiene	Butane
Butylene	Chlorine
Chlorosulfonic acid	Crotonaldehyde
Dimethylamine	Ethane
Ethyl Chloride	Ethylamine
Ethylene	Ethylene chlorohydrin
Ethylene Cyanohydrine	Ethylene dibromide
Ethylene Oxide	Methylacetylene-propadiene mixture
Methacrylonitrile	Methyl Bromide
Methane (LNG)	Methyl Chloride
Oleum (fuming sulfuric acid)	Propane (LPG)
Propylene	Propylene Oxide
Sulfur Dioxide	Vinyl Chloride

(c) Cargoes listed under 46 CFR Chapter I, Subchapters D and O.

**9600 FMSC Annexes**

**9610 Marine Safety Office Chicago**

**9620 Marine Safety Office Huntington**

**9630 Marine Safety Office Louisville**

**9640 Marine Safety Office Memphis**

**9650 Marine Safety Office Mobile**

**9660 Marine Safety Office Paducah**

**9670 Marine Safety Office Pittsburgh**

**9680 Marine Safety Office St. Louis**

**9690 Marine Safety Unit Baton Rouge**

**9700 Glossary of Terms**

<b>ACOE</b>	U. S. Army Corps of Engineers (sometimes referred to as USACE).
<b>ACP</b>	Area Contingency Plan (for Oil and HAZMAT spill response).
<b>AIS</b>	Automated Information System: A shipboard broadcast system, which acts as a transponder providing positional and other information to a remote receiver.
<b>AMS</b>	Area Maritime Security.
<b>AMS Assessment</b>	An analysis that examines and evaluates the infrastructure and operations of a port, taking into account possible threats, vulnerabilities, existing protective measures, procedures, and operations.
<b>AMS Committee</b>	A committee established under 33 CFR Part 103 that assists in the development, review, and update of the Area Maritime Security Plan.
<b>AOR</b>	Area of Responsibility: A Coast Guard area, district, marine inspection zone or FMSC zone described in 33 CFR 3.
<b>ATAC</b>	Anti-Terrorism Advisory Council (chaired by U.S. Attorney's offices).
<b>AWO</b>	American Waterways Operators (industry association).
<b>Asset</b>	Any natural or man-made feature that has value, such as: buildings, vessels, bridges, communication resources, waterways, roads, railroads, cargo facilities, port infrastructure, personnel and equipment, etc.
<b>BNTM</b>	Broadcast Notice To Mariners: A broadcast made by the Coast Guard over marine band VHF-FM to provide navigation safety information to mariners.
<b>Breach of Security</b>	An incident, that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded, or violated.
<b>CBRN&amp;E</b>	Chemical, Biological, Radiological, Nuclear & Explosive.
<b>CDC</b>	Certain Dangerous Cargo, as defined in 33 CFR 160.204
<b>CFR</b>	Code of Federal Regulations: The compilation and codification of U.S. administrative law by subject matter arranged in numerical titles.
<b>Consequence</b>	The estimation of adverse effect from the target/attack scenario; an important consideration in risk evaluation and security planning.
<b>Consequence Management</b>	Measures to protect public health and safety, restore essential government services, and provide emergency relief to governments, businesses, and individuals affected by the consequences of terrorism.
<b>CONPLAN</b>	The Interagency Domestic Terrorism Concept of Operations Plan.
<b>COTP</b>	Captain of the Port: The Coast Guard officer designated by the Commandant, U.S. Coast Guard, to direct Coast Guard law enforcement activities within a designated area of responsibility. A Captain of the Port enforces regulations for the protection and security of vessels, harbors, waterfront facilities, anchorages, bridges, safety and security zones, ports and waterways.
<b>Counter-terrorism</b>	The full range of activities directed against terrorism, including preventive, deterrent, response and crisis management efforts.
<b>Covered Person</b>	A person who may be allowed to have access to Sensitive Security Information. See Section 3520 for a detailed description.

<b>Critical Asset</b>	Any facility, equipment, service or resource considered essential to DOD operations in peace, crisis and war and warranting measures and precautions to ensure its continued efficient operation, protection from disruption, degradation or destruction, and timely restoration.
<b>CSO</b>	Company Security Officer: The person designated by a Company as responsible for the security of the vessel, including implementation and maintenance of the vessel security plan, and for liaison with their respective vessel or facility security officer and the Coast Guard.
<b>Dangerous Substances And Devices</b>	Any material, substance, or item that reasonably has the potential to cause a transportation security incident.
<b>DHS</b>	Department of Homeland Security: The Homeland Security Act of 2002 established the Department of Homeland Security whose primary mission is to prevent, protect against, and respond to acts of terrorism on our soil.
<b>DOD</b>	Department of Defense.
<b>DOS</b>	Declaration of Security: An agreement executed between the responsible Vessel and Facility Security Officers, or between Vessel Security Officers in the case of a vessel-to-vessel activity, that provides a means for ensuring that all shared security concerns are properly addressed and security will remain in place throughout the time a vessel is moored to the facility or for the duration of the vessel-to-vessel activity, respectively.
<b>DOT</b>	Department of Transportation.
<b>EMA</b>	Emergency Management Agency.
<b>EMS</b>	Emergency Medical Services.
<b>EOC</b>	Emergency Operations Center.
<b>Facility</b>	Any facility, whether USCG regulated or non-regulated, situated in, on, under or immediately adjacent to a navigable waterway.
<b>Facility Security Assessment</b>	A self analysis that examines and evaluates the infrastructure and operations of the facility taking into account possible threats, vulnerabilities, consequences, and existing protective measures, procedures and operations.
<b>Family of plans</b>	Concept for a collective group of plans for ports, vessels and facilities.
<b>FBI</b>	Federal Bureau of Investigation: The FBI's duties include protecting the U.S. from terrorist attacks, from foreign intelligence operations, and from cyber-based attacks and high-technology crimes. The FBI normally assumes the role of Lead Federal Agency for response to terrorist incidents.
<b>Federal Register</b>	A daily publication in which U.S. administrative agencies publish both proposed regulations for public comment and final regulations.
<b>FEMA</b>	Federal Emergency Management Agency.
<b>Fleet of Responsibility</b>	The vessels and facilities regulated under 33 CFR Parts 104 and 105 within an FMSC zone.
<b>FMSC</b>	Federal Maritime Security Coordinator: Each Coast Guard Captain of the Port is designated as the FMSC for his/her zone. The FMSC is authorized to establish, convene, and direct the Area Maritime Security Committee; appoint members to the AMS Committee; develop and maintain, in coordination with AMS Committee, the AMS Plan; and implement and exercise the AMS Plan.
<b>FOSC</b>	Federal On Scene Coordinator.
<b>FOUO</b>	For Official Use Only (used by the Federal Government for unclassified operational sensitive documents).

<b>FRP</b>	Federal Response Plan (being replaced by National Response Plan).
<b>FSO</b>	Facility Security Officer: The person designated as responsible for the development, implementation, revision and maintenance of the facility security plan and for liaison with the FMSC and Company and Vessel Security Officers.
<b>HDPA</b>	High Density Population Area. For purposes of this plan, cities or events with a population of more than 100,000 people.
<b>HSAS</b>	Homeland Security Alert System.
<b>HSPD</b>	Homeland Security Presidential Directive: Homeland Security Presidential Directive that shall record and communicate presidential decisions about the homeland security policies of the United States.
<b>IAIP</b>	Information Analysis and Infrastructure Protection Directorate of DHS.
<b>IC</b>	Incident Commander under ICS.
<b>ICS</b>	Incident Command System: Used to manage an emergency incident or a non-emergency event. It can be used for both small and large situations. The system has considerable internal flexibility and can grow or shrink to meet differing needs. This makes it a very cost-effective and efficient management system that can be applied to a wide variety of emergency and non-emergency situations.
<b>ICS/UC</b>	An Incident Command System utilizing a Unified Command (UC) to coordinate multiple agencies/jurisdictions.
<b>IRPT</b>	Inland River Ports and Terminals (industry group).
<b>IRVMC</b>	Inland Rivers Vessel Movement Center.
<b>ISPS Code</b>	International Ship and Port Facility Security Code: the international standard for maritime security. MTSA is the U.S. implementation of the ISPS.
<b>JTTF</b>	Joint Terrorism Task Force (chaired by FBI).
<b>Jurisdiction</b>	The government's right to exercise legal authority over its persons, vessels, and territory. Within the context of MLE, jurisdiction is comprised of three elements: substantive law, vessel status/flag, and location.
<b>Key Port Areas</b>	Areas within ports or along navigable waterways where heavily populated areas, DOD assets, choke points, or vital infrastructure may be vulnerable to attacks.
<b>Layered Maritime Security</b>	System of diverse activities designed to provide multiple opportunities to prevent successful terrorist attacks.
<b>LE</b>	Law Enforcement.
<b>LFA</b>	Lead Federal Agency: The agency designated by the President to lead and coordinate the overall Federal response is referred to as the LFA and is determined by the type of emergency. In general, an LFA establishes operational structures and procedures to assemble and work with agencies providing direct support to the LFA in order to provide an initial assessment of the situation; develop an action plan; monitor and update operational priorities; and ensure each agency exercises its concurrent and distinct authorities under U.S. law and supports the LFA in carrying out the President's relevant policy. Specific responsibilities of an LFA vary according to the agency's unique statutory authorities.
<b>Local Agency</b>	County, city, municipal, etc.
<b>MARAD</b>	Maritime Administration.
<b>MARSEC</b>	Maritime Security.

<b>MARSEC Directive</b>	An instruction issued by the Commandant, or his/her delegate, mandating specific security measures for vessels and facilities that may be involved in a transportation security incident.
<b>MARSEC Level</b>	<p>A three tiered threat alert system consistent with the DHS Homeland Security Alert System (HSAS). The three-level MARSEC system is separate from, yet used in conjunction with, the HSAS system. MARSEC Levels will be set based on maritime interests and may not always correlate to the HSAS. The international community is also using a three-tiered alert system that is consistent with the MARSEC levels used by the Coast Guard.</p> <ul style="list-style-type: none"> <li>• <b>MARSEC 1</b> – Corresponds to HSAS Threat Conditions Green, Blue, and Yellow. It is the level for which minimum appropriate protective security measures shall be maintained at all times.</li> <li>• <b>MARSEC 2</b> – Corresponds to HSAS Threat Condition Orange. It is the level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident.</li> <li>• <b>MARSEC 3</b> – Corresponds to HSAS Threat Condition Red. It is the level for which further specific protective security measures shall be maintained for a limited period of time when a transportation security incident is probable or imminent, although it may not be possible to identify the specific target.</li> </ul>
<b>MDA</b>	Maritime Domain Awareness: Comprehensive information, intelligence, and knowledge of all relevant entities within the U.S. maritime domain – and their respective activities that could affect America’s security, safety, economy, or environment. MDA provides operational forces with an understanding of what is normal in order to increase the likelihood of spotting the abnormal or unusual when it occurs.
<b>MHS</b>	Maritime Homeland Security: MHS is a federal law enforcement mission carried out by domestic law enforcement authorities, including the Coast Guard, and shall be conducted in accordance with settled law enforcement procedures and policies.
<b>Mitigation</b>	The sustained actions taken to reduce or eliminate long-term risk from hazards and their effects.
<b>MMD</b>	Merchant Mariner Document.
<b>MOA</b>	Memorandum of Agreement.
<b>MSD</b>	USCG Marine Safety Detachment.
<b>MSO</b>	USCG Marine Safety Office.
<b>MTS</b>	Marine Transportation System: Consists of waterways, ports and intermodal connections, vessels, vehicles, and system users, as well as federal maritime navigation systems.
<b>MTSA</b>	Maritime Transportation Security Act of 2002: Landmark legislation passed by the 107th Congress to increase the security efforts of the Coast Guard and other agencies in the U.S. Maritime Domain.
<b>Navigable Waters</b>	Those waters shoreward of 12 NM from the baseline, including internal waters subject to tidal influence and those waters not subject to tidal influence that are or have been used, or susceptible of use, as highways for substantial interstate or foreign commerce, or capable of improvement at a reasonable cost to serve as highways for substantial interstate or foreign commerce. Each Coast Guard District maintains a current list of navigable waters of the U.S. within that District.
<b>Need To Know</b>	The critical factor in determining whether a “Covered Person” is allowed access to Sensitive Security Information. See Section 3540 for a detailed description.

<b>NIMS</b>	National Incident Management System: A system mandated by HSPD-5 that provides a consistent nationwide approach for Federal, State, and local governments to work effectively and efficiently together to prepare for, respond to, and recover from domestic incidents, regardless of cause, size, or complexity. To provide for interoperability and compatibility among Federal, State and local capabilities, the NIMS includes a core set of concepts, principles, and terminology. HSPD-5 identifies these as the incident command system; multi-agency coordination systems; unified command; training; identification and management of resources (including systems for classifying types of resources); qualifications and certifications; and the collection, tracking, and reporting of incident information and incident resources.
<b>NRC</b>	National Response Center.
<b>NM</b>	Nautical Mile.
<b>NORTHCOM</b>	U.S. Northern Command.
<b>NRP</b>	National Response Plan: A plan mandated by HSPD-5 that integrates Federal Government domestic awareness, prevention, preparedness, response, and recovery plans into one all-discipline, all-hazards plan.
<b>NVIC</b>	U.S. Coast Guard Navigation and Vessel Inspection Circular.
<b>OPSEC</b>	Operational Security: a process that protects information about capabilities and intentions by identifying, controlling, and protecting evidence of planning and execution of sensitive activities and operations.
<b>PAF</b>	Public Access Facility: An area, designated by the Captain of the Port, with public access that is primarily used for recreation or entertainment purposes, and which primary purpose does not include receiving or servicing vessels regulated under 33 CFR 104.
<b>Physical Security</b>	That part of security concerned with physical measures to safeguard personnel, to prevent unauthorized access to equipment, facilities, material and documents, and to safeguard them against espionage, sabotage, damage, and theft.
<b>Port</b>	A geographic area, either on a seacoast, lake, river or any other navigable body of water, which contains one or more publicly or privately owned terminals, piers, docks, or maritime facilities, which is commonly thought of as a port by other government maritime-related agencies.
<b>Port Security</b>	The safeguarding of vessels and critical assets within a port from internal threats such as destruction, loss, or injury from sabotage or other subversive acts, accidents, thefts, or other causes of a similar nature.
<b>Positive Control Measures</b>	Where intelligence or other information indicates a possible internal threat to the vessel, FMSCs may implement positive control measures intended to enhance the internal security of the vessel and to ensure that the vessel remains under the control of appropriate shipboard authorities (i.e., master and pilot), particularly while the vessel transits critical or vulnerable areas of the port.
<b>PSRAT</b>	Port Security Risk Assessment Tool, a risk assessment tool used by the USCG.
<b>PVA</b>	Passenger Vessel Association (industry group).
<b>QRC</b>	Quick Response Card: a type of checklist commonly used by the Coast Guard to facilitate gathering accurate and complete information regarding an incident during the initial notification and response phase.
<b>Red Flag</b>	A tank barge carrying hazardous materials.
<b>Restricted Areas</b>	The infrastructures or locations identified in an area, vessel, or facility security assessment or by the operator that require limited access and a higher degree of security protection.
<b>Risk</b>	Expected losses over time: Risk = Threat x Vulnerability x Consequence.

<b>RNA</b>	Regulated Navigation Area.
<b>Safety Zone</b>	A designated water or shore area to which access is limited to persons, vehicles, vessels, or objects authorized by the FMSC. It may be stationary and described by fixed limits or it may be described as a zone around a vessel in motion.
<b>Screen</b>	A reasonable examination of persons, cargo, vehicles, or baggage for the protection of the vessel, its passengers and crew. Such screening is intended to ensure that dangerous substances and devices, or other items that pose a real danger of violence or a threat to security are not present.
<b>Security</b>	A condition that results from measures established to protect designated information, personnel, systems, components and equipment against hostile persons, acts, or influences.
<b>Security Inspection</b>	A USCG inspection of a vessel or facility to verify compliance with its approved security plan.
<b>Security Spot Check</b>	A USCG or multi-agency visit to a facility or vessel to verify compliance with all or part of its approved security plan for the current security condition.
<b>Security Survey</b>	An on-scene examination and evaluation of the physical characteristics of a vessel or facility, and its security systems, processes, procedures, and personnel.
<b>Security Zone</b>	A designated areas of land, water, or land and water established for such time as the FMSC deems necessary to prevent damage or injury to any vessel or waterfront facility, to safeguard ports, harbors, territories, or waters of the United States, or to secure the observance of the rights and obligations of the United States.
<b>SSI</b>	Sensitive Security Information: Information within the scope of 49 CFR Part 1520. See Section 3500 for a detailed discussion of SSI.
<b>Threat</b>	A measure of the likelihood of an attack based on maritime domain awareness and the existence of intelligence.
<b>TRANSCOM</b>	U. S. Transportation Command.
<b>TSI</b>	Transportation Security Incident: A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area.
<b>TSA</b>	Transportation Security Administration.
<b>TSAC</b>	Towing Safety Advisory Committee (industry group).
<b>UMIB</b>	Urgent Marine Information Bulletin: a Coast Guard document distributed to waterways users providing urgent navigation safety information.
<b>USCG</b>	United States Coast Guard.
<b>Vessel</b>	Every description of watercraft or other artificial contrivance used, or capable of being used, as a means of transportation on water.
<b>VSO</b>	Vessel Security Officer: The person onboard the vessel, accountable to the Master, designated by the Company as responsible for security of the vessel, including implementation and maintenance of the Vessel Security Plan, and for liaison with the Facility Security Officer and the vessel's Company Security Officer.
<b>Vulnerability</b>	Measures the conditional probability of success given that a threat scenario occurs. It evaluates the adequacy and effectiveness of safeguards (both existing and proposed).
<b>Waterfront Facilities</b>	Piers, wharves, docks, or similar structures to which vessels may be secured and naval yards, stations, and installations, including ranges; areas of land, water, or land and water under and in immediate proximity to them; buildings on them or contiguous to them and equipment and materials on or in them.

- WMD**            Weapon of Mass Destruction: Any weapon or device that is intended, or has the capability, to cause death or serious bodily injury to a significant number of people through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; a disease organism; or radiation or radioactivity.
- WR**              Western Rivers region of the Eighth Coast Guard District. In the context of this plan, the region also encompasses the Illinois River portion of the COTP Chicago zone in the Ninth Coast Guard District.
- WRAMSPC**      Western Rivers Area Maritime Security Planning Committee.

**TAB A: COMMUNICATING SECURITY INFORMATION (FACILITIES)**

<b>Method</b>	<b>Pro's</b>	<b>Con's</b>	<b>Type of info effective for</b>
NRC notification number	Single point of contact.	Designed to report suspicious activities, not security emergencies. Intensive reporting requirement.	Reporting suspicious activity.
911	Readily available in most areas. Linkage to translators for multi-lingual calls. Well-known.	1-way. Not full coverage. System overload.	Incoming notifications to authorities of suspicious activities or emergencies.
IAIP (Information Analysis & Infrastructure Protection division of DHS)	Targeted to users that need the info. Accepts reports.	Seems to have a focus on cyber security, however IAIP has expanded their scope to Maritime and Aviation Security.	
Qualified Individual (QI)	Existing, recognized system. Tested system.		
US ACOE Lockmaster	Back-up if other systems fail – communicate to Lockmaster at next lock.	Limited availability – only where locks exist.	
Use of code words (both positive and negative code words)	Secure. Minimal cost. Can be used under duress in many cases. Can be used onboard vessel for crew, or to dialog back to home office or to agencies.	Not used everywhere. Requires training and awareness. Security could be compromised.	

**TAB B: COMMUNICATING SECURITY INFORMATION (COMMERCIAL VESSELS)**

<b>Method</b>	<b>Pro's</b>	<b>Con's</b>	<b>Type of info effective for</b>
E-mail	Mass distribution. Reliable. Handles lots of info. 2-way comms.	Need a computer or other device to receive. Keeping e-mail addresses updated. Not necessarily immediate. Passive – you usually have to look for it. Might not be secure.	General security information. Can be used to communicate threat levels and other info (must be supplemented by other methods due to passive issue).
Satellite (voice and data).	Reliable. Transmission secure.	Can be blocked in some areas by topography. Not redundant – a system goes down, you might lose coverage. Expensive.	Can be used for just about anything as long as it is working. In data format, can be used for broad distribution.
VHF Radio	Widely available. Immediately available. 2-way. Economical.	Short range – line of sight, although repeaters can be used. Not secure (generally). No guaranteed delivery - not everyone has it or monitors it at all times. Relies on someone recording what they hear over the VHF.	Can communicate any info needed, provided not SSI.
UHF Radio	Often used for search and rescue and/or emergency response.	Longer range than VHF, but range can be limited – repeaters can be used to extend range. Limited pool/availability of users.	Same as VHS.
RACES (HAM operated system)	Long range. Reliable.	Not secure. Limited resources. System has to be activated.	Back-up communications system. Not a primary system for communicating threats.
EPIRB	Self-activating system “after the fact”. Provides location.	Used for distress and providing location, but does not provide the cause of the problem. One-way only.	Could alert authorities that a vessel is in distress (responders need to be aware that it could now be a security issue).
Cellular Telephone	Widely available. Inexpensive.	Limited range. Not reliable. Not secure. System prone to overload. Can't be used for mass or batch communications.	Can be used with computers. One of most effective ways to communicate immediate changes.
Pagers	Widely available. Inexpensive. Can be 2-way and guaranteed delivery.	May not be 100% coverage. Not necessarily reliable. Not secure. Messages can be delayed. Land-based system.	Short informational bulletins. Must be supplemented by other means to insure notification.

Method	Pro's	Con's	Type of info effective for
Landline (telephone)	Widely available in buildings. Generally reliable. Can be made secure.	Not available on vessels. Can be overloaded. Person being called may not be in to receive call/message.	Anything, but may need to be supplemented by other means if not successful.
Fax	Widely available. Generally reliable. Can be made secure. Can broadcast fax.	Can be overloaded. No guarantee fax is picked-up by someone.	Anything, but may need to be supplemented by other means. Particularly effective for broadcast fax. Robust systems exist with additional options.
Internet web sites	Easily accessible. Can be made secure. Can share large amounts of information.	May be difficult to manage access. Passive - Have to know to go look.	Can be used to verify current threat level. Can be used for general interest info (non-SSI). Can provide greater detail once stakeholders informed to go look.
AIS	Navigational tool for vessels and VTS. Can be used to identify location of vessels in the area.	Could be used by terrorists if they obtain the equipment. Local system with limited range. Need the equipment to use it – costly. Some of same limitations of VHS.	A navigational tool that enhances Maritime Domain Awareness, allows for the efficient exchange of vessel traffic information.
Navigational aids (lights, buoys, etc.)	Readily visible for a local area.	Not every waterway user understands what they mean. Upkeep and maintenance. Slow deployment process. Can be affected by waterway conditions (high or low water/flow).	Can be used to designate security zones, RNA's, etc.
First Mate, produced by GENMAR	Essentially "On Star" for marine vessels – provides similar functionality. Relatively new, but not overly expensive.	Developed for US recreational use only. May have similar limitations to satellite.	May be used for security, tracking, and notification of boats in an affected area. May be an effective tool for reporting an emergency. Need to outreach to the company so that they know who to notify.
EAS (Emergency Alert System) and TV/Radio broadcast systems	Wide dissemination of info. Recognized system for the public. Widely available.	No guarantee of delivery. Land-based, limited area of delivery. Not for SSI info.	Can be used to alert local areas for emergency notifications.
Local area systems (CAN – Community alert networks, Reverse 911, sirens, CAER systems, etc.)	Provide saturated, local, targeted coverage. Can identify who has been notified, but not that they understood the message.	Very localized. Subject to system failures. Not available everywhere. Have to answer phone to receive message. Do "zappers" defeat the incoming calls?	Can be used to alert local areas for emergency notifications.

Method	Pro's	Con's	Type of info effective for
US ACOE system for communicating between locks	Very fast and effective system. Standalone hard-wired radio repeater system (VHF and UHF).	Limited access. If other systems down, have to get to ACOE system (physically go there) to communicate. System life in question. Similar "cons" as listed for UHF/VHF communications.	Back-up communications for USCG and others during an emergency.
WATERCOM – Waterways communication system by MOBEX	Existing system. Covers about 90% of inland waterways.	Short life remaining (may be shut down within 5 years). Limited area of coverage. Expensive.	Use to communicate with vessels that have the equipment installed.
Marine Exchange (clearinghouse for marine information)	Central comms clearinghouse between gov't and industry.	Not in all ports. Not-for-profit, so has to be a cooperative effort to use it. Voluntary use.	Communicate between agents, vessel owners, operators, facility owners, port authorities, etc.
Secure VCT for DHS to state Emergency Management directors	Secure phone/fax between DHS and state EM directors.	In developmental stages. Limited access to info. Not sure how EM directors will route info down to industry.	Can be used to disseminate info to state officials. State officials could disseminate further.
Secure gov't comms.	Secure. Limited access.	Limited access. Not available to industry.	Secondary and tertiary comms networks if local networks/systems fail.
Trunked Systems	Moderately secure. Can patch system to VHF/UHF (additional cost).	Not everyone uses the same systems. Relatively short range. Systems can get overloaded. Probably can't be used to call 911.	Similar to VHF, but with limited/restricted accessibility.
Amber Alert System	Public system. Fast and efficient. Thorough.	Passive, 1-way system. Not designed for security. Limited resources in rural areas.	Can be used to communicate threat levels, non-SSI info. Communicate info in an emergency.
NOAA Tone Alert (Weather Radio)	Wide availability. System is readily expandable.	Passive, 1-way system. Not everyone has receivers. Not designed for security. Limited audience.	Can be used to communicate threat levels, non-SSI info. Communicate info in an emergency.

**TAB C: SECURITY REPORTS & QUICK RESPONSE CARD TEMPLATES**

Quick Response Card (QRC) Templates for reporting and responding to Suspicious Activities, Breaches in Security, Transportation Security Incidents, Bomb Threats and Hostage Situations are provided on the following pages. FMSCs may modify the templates for local use by inserting appropriate contacts and telephone numbers.



## Western Rivers Area Maritime Security Plan



### Suspicious Activity Report Form

Suspected Activity _____	MARSEC Threat Level - 1 2 3 _____
_____	Responding Agency _____
Date/Time of Activity _____	Responding Officer/Agent _____
Date Report Made _____	Responding Agency Case No. _____
Reporting Party _____	Responding Agency's Address (physical & e-mail) _____
Reporting Party's Phone No. _____	_____
Responding Agency's Phone _____	_____

Contact Officer/Agent: _____	Contact Phone #s _____
Cell _____	Pager _____
Fax _____	

<b>SUBJECT(S)</b>	
1. Name _____	Sex: _____ Race/Ethnicity _____
Address _____	
DOB _____	SSN _____ Alien# _____
Telephone# _____	
Physical Description _____	
Vehicle: _____	Alias Name _____
2. Name _____	Sex _____ Race/Ethnicity _____
Address _____	
DOB _____	SSN _____ Alien# _____
Telephone#s _____	
Physical Description _____	
Vehicle: _____	Alias Name _____

<b>Vessel / Facility Information</b>	
1. Vessel / Facility Name: _____	Location: (River & mile) _____
Address _____	
Cargo Type & Amount: _____	Number of Barges & Config. _____
POC: _____	Phone: _____
Other Information: _____	

<b><u>SUSPICIOUS ACTIVITY</u></b>
(provide as much detailed information as possible-use additional sheets if needed)

**QRC ACTION CHECKLIST – Suspicious Activity**

<b>Notify:</b>	<b>YES</b>	<b>NO</b>	<b>TIME/DATE</b>	<b>OTHER</b>
Internal Security Staff	___	___	_____	_____
Local LE	___	___	_____	_____
Emergency Svcs	___	___	_____	_____
FMSC / COTP	___	___	_____	_____
NRC	___	___	_____	_____
FBI / JTTF	___	___	_____	_____
State Police	___	___	_____	_____

Contact Information: Agency & Phone numbers:

<b>FBI</b>		
<b>USAO</b>		
<b>USCG</b>		
<b>NRC 800-424-8802</b>		
<b>TSA</b>		

**Initial Actions:**

<b>Security Staff / Local LE investigation</b>	___	___	_____	_____
<b>FBI Threat Assessment</b>	___	___	_____	_____
<b>FMSC determine scope / severity</b>	___	___	_____	_____
<b>Actions to maintain site security</b>	___	___	_____	_____
<b>FMSC Coord. Additional LE response</b>	___	___	_____	_____

**Additional security measures for potentially affected entities:**

<b>Notify District</b>	___	___	_____	_____
<b>Notify GROUP OPCEN &amp; IRVMC</b>	___	___	_____	_____
<b>Share info w/AMSC &amp; Port Stakeholders</b>	___	___	_____	_____
Arrange:	FOSC	___	___	_____
	Firefighting	___	___	_____
Underway:	Boat	___	___	_____
	Helo	___	___	_____
Establish	Safety Zone	___	___	_____
	Security Zone	___	___	_____
	COTP Order	___	___	_____
	Restricted Airspace	___	___	_____
Messages:	Field Intel Rpt	___	___	_____
	BNTM	___	___	_____
	SITREP/POLREP	___	___	_____
	Req. Resources	___	___	_____
Case Info:	Statements	___	___	_____
	Photos	___	___	_____

**Other actions taken:**

# SENSITIVE SECURITY INFORMATION (When filled in)



## Western Rivers Area Maritime Security Plan Breach of Security Report Form



Security Breach _____ Date/Time of Activity _____ Date Report Made _____ Reporting Party _____ Reporting Party's Phone No. _____ _____ Responding Agency's Phone _____	MARSEC Threat Level - 1 2 3 Responding Agency _____ Responding Officer/Agent _____ Responding Agency Case No. _____ Responding Agency's Address (physical & e-mail) _____
------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------	---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------

Contact Officer/Agent: _____	Contact Phone #s _____
Cell _____	Pager _____
Fax _____	

<b>SUBJECT(S)</b>	
1. Name _____	Sex: _____ Race/Ethnicity _____
Address _____	
DOB _____	SSN _____ Alien# _____
Telephone# _____	
Physical Description _____	
Vehicle: _____	Alias Name _____

<b>Vessel / Facility Information</b>	
<b>TYPE</b> (Towboat, Passenger, Barge 126, 127, 154, Passenger, CDC, Barge Fleeting)	
1. Vessel / Facility Name/ Owner: _____	Type: _____
Address _____	Location: (River & mile) _____
Cargo Type & Amount: _____	Number of Barges & Config. _____
POC: _____	Phone: _____
Other Information: _____	

<b><u>SECURITY BREACH</u></b>
<b>Security Measures circumvented, eluded or violated:</b> (provide as much detailed information as possible-use additional sheets if needed)
<b>Actions taken to maintain / restore security at site:</b>
<b>Potential consequences of the Security Breach:</b>

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR 1520.5, except with the written permission of the Secretary of Homeland Security. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR Part 1520.

# SENSITIVE SECURITY INFORMATION (When filled in)

## QRC ACTION CHECKLIST – Security Breach

Notify:	YES	NO	TIME/DATE	OTHER
Internal Security Staff	___	___	_____	_____
Local LE	___	___	_____	_____
Emergency Svcs	___	___	_____	_____
FMSC / COTP	___	___	_____	_____
NRC	___	___	_____	_____
FBI / JTTF	___	___	_____	_____
State Police	___	___	_____	_____

Contact Information: Agency & Phone numbers:

<b>FBI</b>		
<b>USAO</b>		
<b>USCG</b>		
<b>NRC 800-424-8802</b>		
<b>TSA</b>		

**Initial Actions:**

Security Staff / Local LE investigation	___	___	_____	_____
FBI Threat Assessment	___	___	_____	_____
FMSC determine scope / severity	___	___	_____	_____
Actions to maintain site security	___	___	_____	_____
FMSC Coord. Additional LE response	___	___	_____	_____

**Additional security measures for potentially affected entities:**

Notify District	___	___	_____	_____
Notify GROUP OPCEN & IRVMC	___	___	_____	_____
Share info w/AMSC & Port Stakeholders	___	___	_____	_____
Arrange:	FOSC	___	___	_____
	Firefighting	___	___	_____
Underway:	Boat	___	___	_____
	Helo	___	___	_____
Establish	Safety Zone	___	___	_____
	Security Zone	___	___	_____
	COTP Order	___	___	_____
	Restricted Airspace	___	___	_____
Messages:	Field Intel Rpt	___	___	_____
	BNTM	___	___	_____
	SITREP/POLREP	___	___	_____
	Req. Resources	___	___	_____
Case Info:	Statements / Photos	___	___	_____

**Other actions taken:**

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this record may be disclosed to persons without a “need to know,” as defined in 49 CFR 1520.5, except with the written permission of the Secretary of Homeland Security. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR Part 1520.



# SENSITIVE SECURITY INFORMATION (When filled in)

## QRC ACTION CHECKLIST – Transportation Security Incident

Notify:	YES	NO	TIME/DATE	OTHER
Internal Security Staff	___	___	_____	_____
Local LE	___	___	_____	_____
Emergency Svcs	___	___	_____	_____
FMSC / COTP	___	___	_____	_____
NRC	___	___	_____	_____
FBI / JTTF	___	___	_____	_____
State Police	___	___	_____	_____

Contact Information: Agency & Phone numbers:

<b>FBI</b>		
<b>USAO</b>		
<b>USCG</b>		
<b>NRC 800-424-8802</b>		
<b>TSA</b>		

**Initial Actions:**

Security Staff / Local LE investigation	___	___	_____	_____
FBI Threat Assessment	___	___	_____	_____
FMSC determine scope / severity	___	___	_____	_____
Actions to maintain site security	___	___	_____	_____
FMSC Coord. Additional LE response	___	___	_____	_____

**Additional security measures for potentially affected entities:**

Notify District	___	___	_____	_____
Notify GROUP OPCEN & IRVMC	___	___	_____	_____
Share info w/AMSC & Port Stakeholders	___	___	_____	_____
Arrange:	FOSC	___	___	_____
	Firefighting	___	___	_____
Underway:	Boat	___	___	_____
	Helo	___	___	_____
Establish	Safety Zone	___	___	_____
	Security Zone	___	___	_____
	COTP Order	___	___	_____
	Restricted Airspace	___	___	_____
Messages:	Field Intel Rpt	___	___	_____
	BNTM	___	___	_____
	SITREP/POLREP	___	___	_____
	Req. Resources	___	___	_____
Case Info:	Statements / Photos	___	___	_____

**Other actions taken:**

**WARNING:** This record contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR 1520.5, except with the written permission of the Secretary of Homeland Security. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR Part 1520.



## Western Rivers Area Maritime Security Plan



### BOMB THREAT Report Form

COMMENTS: The FBI and local police departments are the primary law enforcement agencies for response to a bomb threat at a facility or a vessel moored thereto. A bomb threat has proven to be one of the most effective weapons used by both terrorists and criminals to cause costly disruptions of normal operations, destruction of property and/or injury or loss of life. Masters, owners/operators of vessels or waterfront facilities are assigned the primary responsibility for protection and security of their vessels or facilities, including protection from bomb threats. The FMSC will assist law enforcement agencies in any way possible.

Be calm and courteous. Listen, do not interrupt caller. Note characteristics of voice. If possible, have someone listen in. The bomb threat call may be traced through traditional means or by using the \*69 call-back function Don't Hang Up!!

<b>INITIAL INFORMATION</b>	Date/Time of Report _____	Reporter _____
What does it look like? _____		
Exact words of person calling: _____		
Name of Threatened Vessel/Facility _____		
Name of Owner/Operator _____		Phone _____
Address of Facility/Location of Vessel _____		
<b>QUESTIONS TO ASK</b>		
When is it set to go off? _____		(unknown)
Where is it? _____		(unknown)
What kind of bomb is it? _____		(unknown)
Why did you place the bomb? _____		(unknown)
Who (what organization) is responsible? _____		(unknown)
<b>DESCRIPTION OF CALLER'S VOICE</b>		
Male/Female _____	Age _____	
Intoxicated _____	Speech Impediment _____	Accent _____
Scripted _____	Ad Lib _____	Recorded _____
<b>BACKGROUND NOISES:</b>		
Music _____	Children _____	Airplane _____
Talk _____	Traffic _____	Typing _____
Machines _____	Boating _____	Fan/Vent _____
Other _____		

**QRC ACTION CHECKLIST – Bomb Threat**

<b>Notify:</b>	<b>YES</b>	<b>NO</b>	<b>TIME/DATE</b>	<b>OTHER</b>
Internal Security Staff	___	___	_____	_____
Local LE	___	___	_____	_____
Emergency Svcs	___	___	_____	_____
FMSC / COTP	___	___	_____	_____
NRC	___	___	_____	_____
FBI / JTTF	___	___	_____	_____
State Police	___	___	_____	_____

Contact Information: Agency & Phone numbers:

<b>FBI</b>		
<b>USAO</b>		
<b>USCG</b>		
<b>NRC 800-424-8802</b>		
<b>TSA</b>		

**Initial Actions:** Notify the Vessel agent/operating company and/or Facility IMMEDIATELY (If not already aware) Inform them NOT to use radios or cell phones. Recommend they evacuate all personnel

**Notify Police Bomb Squad** \_\_\_\_\_  
**Notify Police Dept. and Fire Dept. via 911** \_\_\_\_\_  
**What assistance is necessary to support the FBI / Police?** \_\_\_\_\_  
**Emergency Safety Zone?** \_\_\_\_\_  
**Small boat assistance in transporting Bomb Squads to vessel?** \_\_\_\_\_  
**Small boat assistance in evacuating personnel?** \_\_\_\_\_

<b>Security Staff / Local LE investigation</b>	___	___	_____	_____
<b>FBI Threat Assessment</b>	___	___	_____	_____
<b>FMSC determine scope / severity</b>	___	___	_____	_____
<b>Necessary actions to maintain site security</b>	___	___	_____	_____
<b>FMSC Coord. Additional LE response</b>	___	___	_____	_____

**Additional security measures for potentially affected entities:**

<b>Notify District</b>	___	___	_____	_____
<b>Notify GROUP OPCEN &amp; IRVMC</b>	___	___	_____	_____
<b>Share info w/AMSC &amp; Port Stakeholders</b>	___	___	_____	_____
Underway:	Boat	___	_____	_____
	Helo	___	_____	_____
Establish:	Safety Zone	___	_____	_____
	Security Zone	___	_____	_____
	COTP Order	___	_____	_____
	Restricted Airspace	___	_____	_____
Messages:	Field Intel Rpt	___	_____	_____
	BNTM	___	_____	_____
	SITREP/POLREP	___	_____	_____
	Req. Resources	___	_____	_____

**Other actions taken:**



## Western Rivers Area Maritime Security Plan



### HOSTAGE SITUATION Report Form

COMMENTS: The FBI and local law enforcement agencies will take the lead action in a response to a hostage situation. The FMSC will provide assistance as necessary, such as the establishment of a Safety Zone.

<b>INITIAL INFORMATION</b>		Date/Time of Report _____	Reporter _____
Notified by _____		Phone _____	
TERRORIST/HOSTAGE INFORMATION:			
Number of Terrorists/Hostages _____		Nationality _____	
Number of Hostage Takers _____		Nationality _____	
Name(s) _____			
Age(s) _____			
Health Conditions _____			
Weapons _____			
Terrorist activity/Demands _____			
_____			
Location _____			
_____			
VESSEL/FACILITY INFORMATION:			
Vessel/Facility _____		Vessel/Facility Type _____	
Lat _____	Long _____	Course/Speed _____	
Port of Origin _____		Destination _____	
OTHER INFORMATION:			
Agencies on scene _____		USCG Resources _____	
Communications _____			
Other Comments _____			
_____			

**QRC ACTION CHECKLIST – Hostage Situation**

Notify:	YES	NO	TIME/DATE	OTHER
Internal Security Staff	___	___	_____	_____
Local LE	___	___	_____	_____
Emergency Svcs	___	___	_____	_____
FMSC / COTP	___	___	_____	_____
NRC	___	___	_____	_____
FBI / JTTF	___	___	_____	_____
State Police	___	___	_____	_____

Contact Information: Agency & Phone numbers:

<b>FBI</b>		
<b>USAO</b>		
<b>USCG</b>		
<b>NRC 800-424-8802</b>		
<b>TSA</b>		

**Initial Actions:**

What assistance is necessary to support the FBI? \_\_\_\_\_

Emergency Safety Zone? \_\_\_\_\_

Small boat assistance for transport of FBI or as weapons platform? \_\_\_\_\_

Small boat assistance in evacuating personnel? \_\_\_\_\_

<b>Security / Local LE investigation</b>	___	___	_____	_____
<b>FBI Threat Assessment</b>	___	___	_____	_____
<b>FMSC determine scope / severity</b>	___	___	_____	_____
<b>Actions to maintain site security</b>	___	___	_____	_____
<b>FMSC coord Additional LE response</b>	___	___	_____	_____
<b>Additional security measures for potentially affected entities:</b>	___	___	_____	_____
<b>Notify District</b>	___	___	_____	_____
<b>Notify GROUP OPCEN &amp; IRVMC</b>	___	___	_____	_____
<b>Share info w/AMSC &amp; Stakeholders</b>	___	___	_____	_____
Arrange: FOSC	___	___	_____	_____
Firefighting	___	___	_____	_____
Underway: Boat	___	___	_____	_____
Helo	___	___	_____	_____
Establish: Safety Zone	___	___	_____	_____
Security Zone	___	___	_____	_____
COTP Order	___	___	_____	_____
Restricted Airspace	___	___	_____	_____
Messages: Field Intel Rpt	___	___	_____	_____
SITREP/POLREP	___	___	_____	_____
Req. Resources	___	___	_____	_____

**Other actions taken:**

**TAB D: SSI NON-DISCLOSURE AGREEMENT****CONDITIONAL ACCESS TO SENSITIVE BUT UNCLASSIFIED INFORMATION  
NON-DISCLOSURE AGREEMENT**

I, \_\_\_\_\_ hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain United States Government documents or material containing sensitive but unclassified information.

I understand and agree to the following terms and conditions:

1. By being granted conditional access to sensitive but unclassified information, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement.
2. As used in this Agreement, sensitive but unclassified information is any information which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Title 5, U.S.C., Section 552a, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.
3. I am being granted conditional access contingent upon my execution of this Agreement for the sole purpose of (identify) \_\_\_\_\_.

This approval will permit me conditional access to certain information, e.g., (circle type(s) of information as appropriate) documents, memoranda, reports, testimony, deliberations, maps, drawings, schematics, plans, assessments, etc.) and/or to attend meetings where such information is discussed or otherwise made available to me. This Agreement will not allow me access to materials, which the Department of Homeland Security has predetermined, in its sole discretion, are inappropriate for disclosure pursuant to this Agreement. This may include sensitive but unclassified information provided to the Department of Homeland Security by other agencies of the United States Government.

4. I will never divulge any sensitive but unclassified information that is provided to me pursuant to this Agreement to anyone unless I have been advised in writing by the Department of Homeland Security that the individual is authorized to receive it. Should I desire to make use of any sensitive but unclassified information, I will do so in accordance with paragraph 6 of this Agreement. I will submit to the Department of Homeland Security for security review, prior to any submission for publication, any book, article, column or other written work for general publication that is based upon any knowledge I obtained during the course of my work on (identify) \_\_\_\_\_

in order for the Dept. of Homeland Security to ensure that no sensitive but unclassified information is disclosed.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of sensitive but unclassified information not consistent with the terms of this Agreement.
6. I hereby agree that when reviewing any official documents containing sensitive but unclassified information, such review will be conducted at a secure facility or under circumstances that will maintain the security protection of such material. I will not be permitted to and will not make any copies of documents or parts of documents to which conditional access is granted to me. Any notes taken during the course of such access will remain at the Department of Homeland Security, to be placed in secure storage unless it is determined by the Department of Homeland Security that the notes contain no sensitive but unclassified information. If I wish to have the notes released to me, Department of Homeland Security officials will review the notes for the purposes of deleting any sensitive but unclassified information to create a redacted copy of the notes. If I do not wish a review of any notes that I make, those notes will remain sealed in secure storage at the Department of Homeland Security.
7. If I violate the terms and conditions of this Agreement, I understand that the unauthorized disclosure of sensitive but unclassified information could compromise the security to the Department of Homeland Security.
8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to sensitive but unclassified information. This may serve as a basis for denying me conditional access to Department of Homeland Security information, both classified and sensitive but unclassified information in the future. If I violate the terms and conditions of this Agreement, the United States may institute a civil action for damages or any other appropriate relief. The willful disclosure of information to which I have agreed therein not to divulge may constitute a criminal offense.

9. Until I am provided a written release by the Dept. of Homeland Security from this Agreement or any portions of it, all conditions and obligations contained in this Agreement apply both during my period of conditional access, which shall terminate at the conclusion of my (identify) \_\_\_\_\_, and at all times thereafter.

10. Each provision of this Agreement is severable. If a court should find any provision of this Agreement to be unenforceable, all other provisions shall remain in full force and effect.

11. I understand that the United States Government may seek any remedy available to it to enforce this Agreement, including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement.

12. By granting me conditional access to information in this context, the United States Government does not waive any statutory or common law evidentiary privileges or protections that it may assert in any administrative or court proceeding to protect any sensitive but unclassified information to which I have been given conditional access under the terms of this Agreement

13. These restrictions are consistent with and do not supersede, conflict with or otherwise alter the employee obligations, rights or liabilities created by Executive Order 12356; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302 (b) (8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents), and the statutes which protect against disclosure that my compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. Section 783(b)). The definitions, requirements, obligations, rights, sanctions and liabilities created by said Executive Order and listed statutes are incorporated into this Agreement and are controlling.

14. My execution of this Agreement shall not nullify or effect in any manner any other secrecy or nondisclosure Agreement which I have executed or may execute with the United States Government.

15. I make this Agreement in good faith, without mental reservation or purpose of evasion.

\_\_\_\_\_  
DATE  
\_\_\_\_\_  
NAME (Last, First, Middle I.)  
This Agreement was accepted by the undersigned on behalf of the Department of Homeland Security as a prior condition of conditional access to sensitive but unclassified information.

\_\_\_\_\_  
DATE  
\_\_\_\_\_  
WITNESSED BY - Department of Homeland Security

U.S. DEPARTMENT OF HOMELAND SECURITY HSIF 4024 (01/2003)  
*This form is not subject to the requirements of P. L. 104-13, "Paperwork Reduction Act of 1995" 44 USC, Chapter 35.*

**TAB E: CONSOLIDATED RECOMMENDED MARSEC MEASURES TABLE**

Summary of MARSEC measures recommended for incorporation by port entities as applicable.

	<b>MARSEC 1</b>	<b>MARSEC 2</b>	<b>MARSEC 3</b>
Monitor Port / Waterfront Areas	<p>Monitor port / waterfront areas, including at night and in times of poor visibility.</p> <p>Properly light access points, restricted areas and vessel decks.</p> <p>Recommend using alarms, CCTV, remote sensors, or security patrols on an irregular routine.</p> <p>Deny access to anyone refusing to submit to security verification.</p> <p>Identify access points to port / waterfront areas and vessels.</p> <p>Ensure security is provided or arranged for unmanned vessels moored at a facility.</p> <p>Search facility moorings/piers/docks for dangerous substances or devices prior to vessel arrival.</p>	<p>Increase detail and frequency of monitoring or patrols of port/waterfront areas, including inspection of people, personal effects and vehicles.</p> <p>Establish dedicated patrolling of facilities and moored vessels.</p> <p>Search waterfront areas for explosives, hazardous or dangerous devices.</p> <p>Increase the intensity and coverage of lighting.</p> <p>Increase the use of surveillance equipment.</p> <p>Assign additional security guards.</p> <p>Implement boat patrols.</p>	<p>Continuously monitor port /waterfront areas to protect against an imminent security incident.</p> <p>Turn on all exterior lighting to fully illuminate the vessel/facility.</p> <p>Turn on all surveillance systems.</p> <p>Conduct underwater hull and pier inspections.</p>
Communications	<p>Establish procedures to share information to allow for more complete knowledge of cargo, people and vessels using port.</p> <p>Establish procedures and means of communicating any threatening acts.</p> <p>Immediately report any suspicious activity or breach of security to the Captain of the Port.</p>	<p>Provide personnel briefings describing possible threats, reporting suspicious activities, and the need for vigilance.</p> <p>Enhance means of communication to ensure immediate availability of resources.</p>	<p>Test internal communications plan, as well as communications with the Captain of the Port and local emergency responders.</p>

	<b>MARSEC 1</b>	<b>MARSEC 2</b>	<b>MARSEC 3</b>
Establish & Control Restricted Areas	<p>Establish restricted areas to control access.</p> <p>Designate the following Restricted Areas (as applicable): navigational bridge; control stations; machinery spaces; access to voids, tanks, and cofferdams; pump rooms; and other spaces deemed to be security sensitive.</p> <p>Clearly define &amp; mark restricted areas.</p> <p>Develop restricted area access control policy, including identification verification and frequency of application.</p> <p>Implement security measures needed to prevent unauthorized access to restricted areas, including but not limited to: lock or secure access points, using monitoring systems, guards or patrols, and remote detection systems.</p> <p>Limit the number of access points to restricted areas.</p> <p>Monitor restricted areas.</p> <p>Erect perimeter barriers or fences.</p> <p>Block window entry using sealed windows, bars etc.</p>	<p>Control access to restricted areas to allow only authorized personnel.</p> <p>Increase frequency and detail of monitoring restricted areas.</p> <p>Establish a dedicated restricted area guard or patrol system.</p>	<p>Continuously monitor restricted areas to protect against an imminent security incident.</p> <p>Restrict access to additional areas that are threatened by a security incident or threat.</p> <p>Regularly search all restricted areas.</p>

	<b>MARSEC 1</b>	<b>MARSEC 2</b>	<b>MARSEC 3</b>
Control Personnel Access	<p>Identify all vehicle traffic and contents entering the facility.</p> <p>Deny access to persons refusing to comply with security measures or without a valid reason to enter the facility or vessel.</p> <p>Provide an employee identification system.</p> <p>Provide a visitor identification system.</p> <p>Establish a designated parking scheme.</p> <p>Allow only authorized personnel and vehicles to have access to facilities/vessels.</p> <p>Pre-schedule vessel arrivals and work conducted to ensure proper access authority has been granted.</p> <p>Randomly screen persons, baggage, and vehicles for dangerous materials that enter the facility or vessel.</p> <p>Screen all unaccompanied baggage prior to facility/vessel entry.</p> <p>Establish visitor escort procedures.</p> <p>Maintain a secure area for screening of baggage and passengers.</p> <p>Segregate embarking and disembarking passengers.</p>	<p>Limit the number of access points to the port/facility/vessel.</p> <p>Increase control of access points to port or other identified areas.</p> <p>Extra staff and security personnel should be available on short notice.</p> <p>Increase random screening of persons and baggage for dangerous substances or devices prior to entering the facility/vessel.</p> <p>Increase random screening of passenger and commercial vehicles prior to entering the facility/vessel.</p> <p>Randomly screen vehicles leaving the facility.</p> <p>Limit parking around sensitive or restricted areas.</p> <p>Use boat patrols to deter waterside access to vessels and facilities.</p>	<p>Limit facility/vessel access to one point of entry.</p> <p>Employ additional security measures at the point of entry to strictly control access to port/waterfront areas and vessels.</p> <p>Screen all persons, baggage and vehicles entering the facility.</p> <p>Screen all unaccompanied baggage for dangerous substances or devices.</p> <p>Perform a full search of the facility or vessel.</p>

	<b>MARSEC 1</b>	<b>MARSEC 2</b>	<b>MARSEC 3</b>
Control Cargo & Ship's Stores Operations	<p>Verify and inspect cargo contents against the cargo's documentation and cargo storage areas.</p> <p>Conduct cargo checks by: visual inspection, physical inspection, scanning equipment, trained dogs, or coordinating security measures with the shipper.</p> <p>Develop inventory control procedures that identify cargo as having been checked and inspected for loading or storage.</p> <p>Develop cargo movement procedures that address cargo handling, receiving, releasing, designated storage, and coordinated with inventory controls.</p> <p>Designate cargo inspection areas as restricted areas.</p> <p>Release cargo only to the authorized carrier, verify all authorized carriers.</p> <p>Conduct routine cargo checks (including cargo spaces) prior to and during cargo operations.</p> <p>Routinely check cargo seals or other anti-tampering devices.</p> <p>Screen vehicles bringing cargo to the facility.</p> <p>Check that ship's stores match the purchase order prior to loading aboard the vessel.</p> <p>Maintain positive control of stores until properly stowed.</p> <p>Supervise handling of cargo and ship's stores.</p>	<p>Increase the frequency and scope of physical cargo and cargo space inspections.</p> <p>Increase frequency and detail of supervising handling of cargo and ship's stores.</p> <p>Increase the frequency of checking seals or other anti-tampering devices.</p> <p>Ensure that only the cargo/stores intended to be loaded are loaded.</p> <p>Limit the number of locations where cargo/stores may enter the facility.</p> <p>Properly store cargo/stores to provide security personnel an unimpeded view, or inspection.</p> <p>Prepare for the suspension or restriction of accepting cargo/stores at the facility.</p>	<p>Check all cargo/stores being brought aboard the facility or vessel.</p> <p>Consider securing cargo and ship's stores operations.</p>

**TAB F: PUBLIC ACCESS FACILITY GUIDANCE**

## (a) Sample Request for Designation as a Public Access Facility:

	Company Letterhead Date
<p>U.S. Coast Guard Marine Safety Office (Name) Attn: Captain of the Port Address City, State, Zip</p> <p>Dear Captain of the Port:</p> <p>We request designation of _____ as a "Public Access Facility" under 33 CFR § 101.105. [Describe why your facility meets the definition of a "public access facility": type of facility, primary use of facility, type and frequency of vessels subject to 33 CFR § 104 that use facility]</p> <p>For your reference, we have conducted an abbreviated facility security assessment. [Include results, which could consist of the following:</p> <ul style="list-style-type: none"> <li>• Enclose diagram showing access points, both land and water</li> <li>• Enclose map of area showing highways, railroads, etc.</li> <li>• Security measures you and/or vessels will take during facility-vessel interface</li> <li>• Enclose photos of facility and surrounding area]</li> </ul> <p>We will implement the following security measures at the various MARSEC levels: [List security measures the facility will follow at MARSEC Levels 1, 2, and 3].</p> <p>The following personnel are responsible for implementing security measures: [Detail primary and alternate points of contact and twenty-four hour contact phone number, fax, and email information].</p> <p>I understand that under 33 CFR § 105.110, the Captain of the Port (COTP) may establish conditions for facility designation as a Public Access Facility to ensure adequate security is maintained. I further understand that under 33 CFR § 105.110, the COTP may withdraw the designation of a Public Access Facility at any time the owner or operator fails to comply with any requirement of the COTP as a condition of the designation or any measure ordered by the COTP.</p> <p>Thank you for your consideration. If you have any further questions, you can reach me at [your contact information].</p> <p style="text-align: center;">Sincerely,</p> <p style="text-align: center;">Security Officer</p>	

(b) Sample Public Access Facility Designation Letter:

<p><i>COTP Letterhead</i></p> <p style="text-align: right;">16600 <i>Date</i></p> <p><i>Facility Owner/Operator</i> <i>Address</i> <i>State</i></p> <p>SUBJECT: PUBLIC ACCESS FACILITY DESIGNATION (<i>COMPANY NAME, FIN, MISLE ID #</i>)</p> <p>I have received your letter of <i>dd/mm/yyyy</i> requesting designation as a Public Access Facility under 33 CFR Subchapter H. Taking into account the provisions of these regulations that allow for certain exemptions, and after evaluating your facility, I have determined that _____ qualifies for designation. Your request for designation is therefore granted subject to continuing compliance with the conditions outlined below:</p> <ul style="list-style-type: none"> <li>• Provide this office appropriate 24-hour contact information for the designated individual with security responsibilities for the Public Access Facility.</li> <li>• Comply with any Maritime Security (MARSEC) measures described in the Area Maritime Security Plan, all measures described in enclosure (1) to this letter, and any Captain of the Port Orders requiring additional security measures.</li> <li>• Report any suspicious activities to the National Response Center at 1-800-424-8802.</li> </ul> <p>As per 33 CFR Part 105.110(d)(3), the Captain of the Port may withdraw the designation of a Public Access Facility at any time the owner or operator fails to comply with any requirement established as a condition of the designation, or any measure ordered by the Captain of the Port.</p> <p>You must be in full compliance with these required measures by July 01, 2004. This designation will be evaluated annually to ensure the conditions remain appropriate. If there are any changes to the use or description of your facility you may be required to prepare and implement a Facility Security Plan in accordance with 33 CFR Part 105.</p> <p style="text-align: right;">Sincerely, <i>COTP Signature Block</i></p> <p>Encl: (1) Required Security Measures for Public Access Facility</p>
<p><b>SENSITIVE SECURITY INFORMATION</b></p> <p>Enclosure (1) to Public Access Facility Designation for _____ <i>List all requirements from AMS Plan and any additional facility-specific requirements</i></p> <p>I acknowledge and accept the conditions of the designation as a Public Access Facility documented in the Coast Guard Captain of the Port letter of <i>mm/dd/yyyy</i>. I will immediately inform the Captain of the Port of any changes of the operations at this facility that may affect this status.</p> <p>Signed: _____ Date: _____ Public Access Facility Owner/Operator</p> <p>Signed: _____ Date: _____ Individual with Security Responsibilities</p> <p>24 Hour contact information: _____</p> <p style="font-size: small;">WARNING: This record contains Sensitive Security Information that is controlled under 49 CFR Part 1520. No part of this record may be disclosed to persons without a "need to know," as defined in 49 CFR 1520.5, except with the written permission of the Secretary of Homeland Security. Unauthorized release may result in civil penalty or other action. For U.S. Government agencies, public disclosure is governed by 5 U.S.C. 552 and 49 CFR Part 1520.</p>

## (c) PAF Security Measures Checklist:

PUBLIC ACCESS FACILITY REQUIREMENTS	Required	Additional Requirements to Review for Applicability
Designate, in writing, by name or by title, an Individual with Security Responsibilities and identify how the officer can be contacted at any time.	X	
Operate in compliance with the approved PAF requirements.	X	
Report to the COTP within 12 hours of notification of an increase in MARSEC Level, implementation of the additional security measures required for the new MARSEC Level.	X	
Determine locations where restrictions or prohibitions to prevent unauthorized access to facility and vessel are to be applied for each MARSEC Level.	X	
Document means of enforcement for each identified restriction or prohibition at each MARSEC level.	X	
Report of all breaches of security, suspicious activities and transportation security incidents IAW AMS plan, Security Incident Procedures and to the National Response Center.	X	
Document security incident procedures.	X	
Document baseline facility security.	X	
An owner or operator whose facility is not in compliance with the requirements of the PAF designation letter must inform the COTP and obtain approval prior to interfacing with an MTSA regulated vessel or continuing operations.	X	
Maintain ability to have effective communications with MTSA regulated vessels to use facility.	X	
Identify procedures for overnight security to accommodate unattended MTSA regulated vessels.		X
Conduct a Facility Security Assessment (FSA) if PAF was identified as location for potential TSI in AMS Assessment.		X
Establish parking procedures and identify designated parking areas, restricting passenger vehicle access to mooring areas.		X
<b>Individual with Security Responsibilities</b>		
Possess knowledge of general vessel and facility operations and conditions.	X	
Possess knowledge of vessel and facility security measures, including the meaning and the requirements of the different MARSEC Levels.	X	
Possess knowledge of emergency response procedures.	X	
Possess knowledge of methods of facility security surveys and assessments.		X
Possess knowledge of handling sensitive security information and security related communications.	X	
Possess knowledge of and must have ability to coordinate security services in accordance with the approved PAF requirements.	X	
<b>MARSEC I</b>		
Maintain baseline security.	X	
<b>MARSEC II (When MTSA regulated vessel at facility)</b>		
Continue MARSEC I requirements.	X	
Notify all facility personnel about identified threats; emphasize reporting procedures and stress the need for increased vigilance.	X	
Implement security requirements for restricted areas.	X	
Ensure the execution of Declarations of Security with Masters, Vessel Security Officers or their designated representatives.	X	
Increase security personnel from baseline.		X
Limit 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.		X
Limit access to restricted areas by providing physical barriers.		X
Ensure adequate security sweeps are conducted to detect dangerous substances or devices.		X

MARSEC III (When MTSA regulated vessel at facility)		
Continue MARSEC II requirements.	X	
Implement security requirements for restricted areas.	X	
When MTSA regulated vessel is at the facility be prepared to implement additional measures including: (1) the use of waterborne security patrols, (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.	X	
Ensure the execution of Declarations of Security with Masters, Vessel Security Officers or their designated representatives.	X	X
Suspend access to the facility.		X
Evacuate the facility.		X
Restrict pedestrian or vehicular movement on the grounds of the facility.		X
Increase security patrols within the facility.		X
Declaration of Security (DOS)		
Each facility owner or operator must ensure procedures are established for requesting a DoS and for handling DoS requests from a vessel.	X	
The effective period of a continuing DoS at MARSEC Level 1 does not exceed 90 days.		X
The effective period of a continuing DoS at MARSEC Level 2 does not exceed 30 days.		X
When the MARSEC Level increases beyond that contained in the DoS, the continuing DoS is void and a new DoS must be executed.	X	
Maintain 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.	X	
Neither the facility nor the vessel may embark or disembark passengers, nor transfer vessel stores until the DoS has been signed and implemented.	X	
The COTP may require, at any time, at any MARSEC Level, any facility subject to this part to implement a DoS with the VSO prior to any vessel-to-facility interface when he or she deems it necessary.		X

**TAB G: RECOMMENDED FMSC OPSEC MEASURES (Limited Distribution)**

Tab G is designated SSI and maintained as a separate document. It may only be distributed within the Coast Guard.