U.S. Department of Transportation
United States Coast Guard

Commandant
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-MPS
Phone: 202-267-0388
FAX: 202-267-4700

COMDTPUB P16700.4
NVIC 9-02 Change 2
27 OCT 2005

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 9-02, Change 2

Subj: GUIDELINES FOR DEVELOPMENT OF AREA MARITIME SECURITY COMMITTEES AND AREA MARITIME SECURITY PLANS REQUIRED FOR U.S. PORTS

Ref: (a) MSM Volume VII, Port Security, COMDTINST M16000.12 (series)
(b) Magnuson Act and Executive order 10173, as amended
(c) Ports and Waterways Safety Act (PWSA) of 1972
(d) Risk-Based Decision-Making, COMDTINST M16010.3 (series)
(e) COMDT COGARD Washington DC 172345 DEC 01
(f) PDD-63 Critical Infrastructure Protection
(g) HSPDD – 3 Homeland Security Advisory System
(h) DOT Report to Congress, "An Assessment of the U.S. MTS" dated Sept. 1999
(i) Navigation and Vessel Inspection Circular No. 1-00, Guidance for the Establishment and Development of Harbor Safety Committees Under the Marine Transportation System (MTS) Initiative, COMDTPUB P16700.4
(j) Navigation and Vessel Inspection Circular No. 10-04, Guidelines for Handling of Sensitive Security Information (SSI), COMDTPUB P16700.4
(k) Guidance for Coast Guard Coordination of MTS Improvement Efforts at the Regional and Local Level, COMDTINST M16010.9 (series)
(l) Interagency Commission on Crime and Security in U. S. Seaports, August 2000
(m) COMDT COGARD Washington DC R281216Z MAY 02/ALCOAST 258/02, G-CCS
(n) CPPM, Volume III; Exercise Policy COMDTINST M3010.13 (series)
(o) Homeland Security Exercise and Evaluation Program, Vol. I-V
(p) National Response Plan, December 2004
(q) Maritime Transportation Security Act, Public Law 107-295; 46 USCA §§ 70101 et. seq.
(r) 33 CFR Subchapter H, Parts 101 – 106.
(s) Alignment with the National Incident Management System and National Response Plan, COMDTINST 16000.27

DISTRIBUTION – SDL No. 140

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B		1	1		1			1						1	1			1								1
C												1														
D	1	1		1							1															
E															1											
F																										
G																										
H																										

*NON-STANDARD DISTRIBUTION: Ba: Commandant (G-MP/G-MOC/MO-1//MSE/MW/OPD/OPL/OPF-3). Distributed by electronic means only.

1. PURPOSE. The purpose of this Circular is to 1) provide guidance to field commanders on the development and maintenance of Area Maritime Security Committees and Area Maritime Security (AMS) Plans; 2) provide guidance on the responsibilities of the Captain of the Port (COTP) acting as the Federal Maritime Security Coordinator (FMSC); 3) provide a common template for AMS Plans; and 4) address port security issues that are the shared responsibility of the port stakeholders and AMS Committees.

2. ACTION. Commanders of Sectors and Activities, and Commanding Officers of Marine Safety Offices and Marine Safety Units will give the guidance in this circular the widest dissemination to the maritime community and AMS Committee members. AMS Committees and AMS Plans should follow the guidance provided in enclosures (1) through (4). This circular will be distributed by electronic means only. It is available on the World Wide Web at http://www.uscg.mil/hq/g-m/nvic/index.htm. Distribution may be made by any practical method.

3. DIRECTIVES AFFECTED. NVIC 9-02, Change 1 is revised to provide guidance on the Final Rules on Maritime Security, 33 CFR Subchapter H, and the Maritime Transportation Security Act (MTSA) of 2002. Enclosures (1) and (2) have been revised. Enclosure (3), the Port Security Risk Assessment Tool, is unchanged and should continue to guide the FMSC with respect to the AMS Assessments. Enclosure (4) is a new addition and provides guidance on the AMS Exercise Program.

4. BACKGROUND.

   a. The terrorist attacks of September 11, 2001, re-awakened the Nation to the reality that it is not isolated from world events and it is vulnerable to terrorist attacks. Since then, numerous reports and studies, including "The Interagency Commission on Crime and Security in U.S. Seaports," have identified the ports, waterways and coastal areas as being particularly vulnerable. The Coast Guard has responded by re-evaluating and strengthening its abilities to protect the Nation's ports, waterways, and coastal areas from possible attack.

   b. International trading partners are an integral part of U.S. security solutions. In November 2001, the Commandant of the Coast Guard addressed the International Maritime Organization (IMO) General Assembly urging that body to consider an international scheme for port and shipping security. As a result, a new international security code, the International Ship and Port Facility Security Code (ISPS), was developed at the Maritime Safety Committee's 75th session in May 2002. In December 2002, the IMO Diplomatic Conference adopted the ISPS Code and a new Chapter XI-2, entitled Special Measures to Enhance Maritime Security.

   c. On November 25, 2002, the President signed into effect Public Law 107-295, the Maritime Transportation Security Act of 2002 (MTSA), that mandated the development of a new regulatory scheme for maritime security. The Coast Guard conducted extensive public outreach, including seven public meetings to request

comment on the development of interim rules to implement the MTSA. More than 2,000 people representing a cross-section of the maritime community attended these meetings and provided extensive comments. The Coast Guard incorporated the public comment into the development of Six Temporary Interim Rules (TIR) that were published in the Federal Register on July 1, 2003. Following another public meeting and the receipt of 1,600 comments from the public, the TIRs were published as Final Rules on October 22, 2003.

5. DISCUSSION.

a. NVIC 9-02, Change 1 provided guidance to FMSCs on how to bring existing Port Security Committees (PSC) and Port Security Plans (PSP) into compliance with 33 CFR Subchapter H, pertaining to the establishment of AMS Committees and AMS Plans. Since June 1st, 2004, forty-six AMSCs have been established. NVIC 9-02, Change 2 is provided to expand and update this guidance.

b. The FMSCs are responsible for establishing and maintaining AMS Committees that advise on the development of an AMS Plan for each COTP zone. The AMS Committees also develop methods to identify risks, communicate threats to affected stakeholders, coordinate resources, and mitigate threats and consequences. Enclosure (1) provides guidelines for the AMS Committees.

c. The AMS Plans and Committees are the cornerstone in bolstering the first lines of defense of our Nation's ports. Their importance cannot be over emphasized. Enclosure (2) provides guidelines for FMSCs in the development and maintenance of AMS Plans and provides the standard AMS plan template. The use of this template is mandatory, as the FMSC and AMS Committees are contributing to the establishment of a Maritime Common Operating Picture (MCOP) that permits critical decision makers to have access to vital information. The AMS Plan is essential to the MCOP as it represents coordinated planning as a joint venture between many departments of the government and civilian community at the port level.

d. The first stage of the AMS Plan process begins with a security assessment of the port area conducted by the FMSC and AMS Committee. Enclosure (3) includes the risk assessment tool that should be used. Further information on risk-based decision-making is available in reference (d). The AMS Plan should provide for coordinated scalable actions to detect, deter, prevent and respond to threats at varying threat levels.

e. The second stage of the planning process includes the actual planning to attempt to mitigate or minimize the risks identified through the port security risk assessment.

f. The following stages in the continuous planning cycle include exercises, evaluation, and amendments. Enclosure (4) provides guidance on the AMS

Exercise Program. Recommendations on port security training are also included in Enclosure (4), but training should be considered an ongoing evolution existing in all stages of the planning process.

g. AMS Plans will contain sensitive security information (SSI) and it is anticipated that AMS Committees will need to access or produce information that is designated as SSI. Once portions of the Plan or its annexes are designated as SSI, the entire Plan should be considered SSI and marked accordingly. However, FMSCs are encouraged to redact SSI information from the Plan so that they may broadly share with the port community those portions of the AMS Plan that are not SSI, e.g., the Communications Section. The SSI program is authorized by Transportation Security Administration (TSA) regulation (reference (m)). Additional guidance is provided in enclosure (2) on the handling, dissemination, and protection of SSI portions of the AMS Plan and AMS Committee minutes.

h. While the guidance contained in this document may assist the industry, public, Coast Guard and other federal and state regulators in applying statutory and regulatory requirements, the guidance is not a substitute for applicable legal requirements, nor is it a regulation itself; thus, it is not intended to, nor does it, impose legally-binding requirements on any party.

6. IMPLEMENTATION.

a. Coast Guard Area and District Commanders will work with FMSCs to establish scalable port security measures based upon the input received from the AMS Committees. These measures may include Regulated Navigation Areas with a port security component, security zones activated only during heightened threat conditions, or other combinations of field regulations issued under 33 CFR Part 165. Ultimately, these preplanned port security measures will allow for quick implementation when MARSEC levels are raised. At no time, however, will these security measures prevent a FMSC from taking more extensive measures, pursuant to existing authority, within their port in times of national emergency or imminent attack.

b. FMSC Responsibility

(1) FMSCs will use the enclosed guidelines to develop and maintain AMS Committees that conform to 33 CFR Subchapter H for Area Maritime Security and the MTSA.

(2) Each FMSC will use the enclosed guidelines to develop and maintain an AMS Plan and an associated exercise program. These plans may include geographic sub-plans as annexes as long as the entire COTP zone is covered.

(3) AMS Plans will be submitted by the FMSC in an electronic format to their District Commander for review in accordance with District direction and Section 8000 of Enclosure (2) of this document.

c. District Responsibility

(1) District Commanders will engage with Sector, Activities, MSO or MSU planners, when necessary, to ensure timelines are met. In doing so, they will provide any technical or drafting assistance needed at the field level.

(2) District Commanders will review all AMS Plans within their District based on the criteria found in enclosure (2), and forward the plans to the appropriate Area Commander based upon their direction.

d. Area Responsibility

(1) Area Commanders will review and approve all AMS Plans in accordance with the criteria found herein, and forward approved AMS Plans to G-MP.

e. Headquarters Responsibility

(1) G-MP will establish and review the policy and doctrine governing the AMS Committees, Plans and Exercises.

T. H. GILMOUR
Assistant Commandant for Marine Safety
Security and Environmental Protection

Encl: (1) Guidance for Development and Management of AMS Committees
(2) Guidance for Development and Management of AMS Plans
(3) Port Level AMS Assessments (PSRAT)
(4) Guidance for Development and Management of an AMS Exercise Program

ENCLOSURE (1) TO NVIC 9-02 CHANGE 2

GUIDANCE FOR DEVELOPMENT AND MANAGEMENT OF AREA MARITIME SECURITY (AMS) COMMITTEES

1. PURPOSE.

   a. The guidance provides information on the purpose, structure, and conduct of AMS Committees and is intended to assist the Federal Maritime Security Coordinators (FMSC) in establishing and maintaining Area Maritime Security (AMS) Committees.

2. BACKGROUND.

   a. Over the last decade, the Captains of the Ports (COTP) have established a broad spectrum of port committees, including Port Readiness Committees, Harbor Safety Committees, Area Committees for Oil and Hazardous Materials Response, Heavy Weather Committees, and other Federal, State, and local committees, to facilitate response to, and promote awareness of, specific incidents within the maritime domain.

   b. COTPs were directed to establish PSCs pursuant to COMDT COGARD Washington DC 172345Z Dec 01. Guidance on the establishment of the PSC was provided in the original NVIC 9-02, dated September 30, 2002. Since that time, the Maritime Transportation Security Act (MTSA) was signed into law, and the Coast Guard issued implementing regulations on area maritime security in 33 CFR Subchapter H. The regulations also implemented a change in terminology from "Port Security" to "Area Maritime Security" for both plans and committees.

   c. Although the MTSA specifically waives the application of the Federal Advisory Committee Act (FACA), 5 U.S.C. App. Sec. 14, to the formation of AMS Committees, each AMS Committee is required to conform to certain provisions in the MTSA, and the procedures established in 33 CFR 103.300. In particular, 103.300 mandates a written charter for the formation of AMS Committees.

3. DISCUSSION.

   a. Establishment of AMS Committees

      (1) The Coast Guard's Ports, Waterways and Coastal Security (PWCS) mission is to deter, detect, prevent and respond to attacks against U. S. territory, population, and critical maritime infrastructure. The mission can best be accomplished through interagency, intergovernmental, and public/private sector cooperative efforts. As the Lead Federal Agency for PWCS, the Coast Guard will accomplish its mission in part through AMS Committees that provide a framework to communicate threats, identify risks, and coordinate resources to mitigate threats and vulnerabilities.

   b. Purpose and responsibilities of the AMS Committees.

      (1) The purpose of the AMS Committee is to assist and advise the FMSC in the development, review and update of an AMS Plan for its COTP zone. It is essential that the Committee, working with the FMSC, develop a plan that contemplates attacks upon its particular infrastructure that would most likely create a Transportation Security Incident (TSI) within its zone. In doing so, the AMS Committee should consider the MTS infrastructure defined in "An

Assessment of the U. S. Marine Transportation System," and in Presidential Decision Directive 63, "Critical Infrastructure Protection."

(2) 33 CFR 103.310 directs the Committees to act as a link in communicating threats and changes in MARSEC levels, a measure meant to address concerns voiced by industry and the boating public about how security and threat information will be communicated and protected. The Communications Section of the AMS Plan template in enclosure (2) is intended to serve as a guide to the FMSCs in the development of communications plans that address those concerns, and in identifying the role of the AMS Committee in the communications process.

(3) PWCS encompasses national security objectives pertaining to the MTS, including the need to support military operations conducted through the ports by the Department of Defense. The AMS Committee is responsible for planning and coordinating security procedures, and is not to be considered a response entity for the purposes of crisis management. However, the links between the AMS Committee and other response-driven entities, such as the DOD, the Area Committee for Oil and Hazardous Materials Response and other existing port committees, are crucial to improving overall preparedness. Just as jurisdictions in the ports are overlapping, some committee responsibilities may overlap. The need for coordination has been directly addressed by the Port Readiness Committees (PRCs) and the National Port Readiness Network (NPRN).

c. Organization of AMS Committees.

(1) When developing the local membership and organization of the AMS Committees, FMSCs should take into account all aspects of the MTS in each port area and its adjacent waterways and coastal areas. The AMS Committees should be comprised of Federal, State, and local agencies, law enforcement and security agencies, and port stakeholders. Representatives for each aspect of MTS and those charged with its regulation or enforcement should be encouraged to participate. For example, AMS Committee membership could include, but is not limited to, representatives from the following agencies:

(i) Federal Agencies:

- US Coast Guard (e.g., Groups, Air Stations , Small Boat Stations, VTS, MSSTs, Auxiliaries);
- Department of Defense (DOD);
- Nuclear Regulatory Commission (NRC);
- US Department of Agriculture (USDA);
- Environmental Protection Agency (EPA);
- Occupational Safety and Health Agency (OSHA);
- Federal Bureau of Investigation;
- Federal Emergency Management Agency (FEMA);
- Customs and Border Protection (CBP);

- Immigration and Customs Enforcement (ICE);
- Transportation Security Administration (TSA);
- Army Corps of Engineers (ACOE);
- US Transportation Command (TRANSCOM);
- Military Sealift Command (MSC);
- Military Traffic Management Command;(MTMC);
- Animal and Plant Health Inspection Service (APHIS);
- Maritime Administration (MARAD);
- Research and Special Programs Administration (RSPA);
- Federal Railway Administration (FRA);
- Federal Highway Administration (FHWA);
- Federal Transit Administration (FTA);
- Other government representatives, where appropriate.

(ii) State and local agencies:

- National Guard;
- Marine Police;
- Port Authority Police and/or security forces;
- Fire Departments;
- Civil Defense;
- City Government officials;
- Transportation agencies;
- Fish and Wildlife marine units;
- Health agencies;
- Occupational safety agencies;
- Terminal/facility security forces;
- Pilot associations;
- Other State, local and City Government representatives;
- State Department of Natural or Environmental Resources marine units;
- Other environmental agencies;
- Regional development agencies/metropolitan planning organizations;

(iii) Industry related agencies:

- Facility owners/operators;
- Terminal owners/operators;
- Trade organizations;
- Recreational boating organizations (Yacht Clubs, rowing clubs);
- Railroad companies;
- Trucking companies;
- Shipyards;
- Tow-boat operators;
- Marine exchanges;
- Industry organizations;

- Organized labor;
- Commercial fishing industry;
- Waterborne vendors & service providers (Harbor Tugs, Launch Services, Line Handlers, small ferry operators, water taxis);
- Other facilities within the port having waterside access, e.g., refineries, chemical plants, power plants.

(2) The MTSA, enacted in 46 USCA 70112(b)(3), requires that before appointing a member to a position on the AMS Committee, notice soliciting nominations for membership on that Committee shall be published in the Federal Register. The COTP/FMSC is likely to be the first to know of pending local AMSC vacancies. It is also apparent that vacancies will occur more frequently than every 3, 4, or 5 years. Therefore, it is more practical for each COTP/FMSC to promulgate membership solicitations as appropriate rather than CG Headquarters promulgating a consolidated notice. A sample AMSC membership solicitation can be found on the G-LRA website under Boilerplate templates, as well as the MTSA website at http://cgweb.comdt.uscg.mil/g-mp/field.html. It is also included as Tab A of this document. If, after the solicitation/application process is complete, a FMSC becomes aware of other individuals or sectors of the port industry that he/she believes should be part of the AMS Committee, it is up to the FMSC to solicit representation from those individuals or sectors. This may be done without any further requirement to publish a notice in the Federal Register. For example, it may be appropriate for the FMSC to solicit federal agency representatives outside the Federal Register process to ensure strong agency representation on the Committee. Also, for those members who may have already been designated in writing by the FMSC as members of AMS Committees, it is not necessary for these members to reapply for their positions.

(3) 33 CFR 103.305(b) requires that at least seven of the members of the AMS Committee each have five years of experience related to maritime or port security operations within the area. The FMSC shall use his/her best judgment in selecting individuals that are best suited as members of the AMS Committee, and in determining if each member's qualifications meet the intent of the regulations.

(4) In accordance with 33 CFR 103.305, each member of the AMS committee shall be appointed for a term of not more than five years. The FMSC shall designate membership terms to ensure that all memberships do not expire within the same year. As such, when establishing the AMS Committee, some members may be designated for only three years, vice five, to provide for continuity of AMS Committee operations. Appointment as a Committee member should be made by formal written document. A sample Invitation, Designation and Acceptance letter is provided at TAB A, B, and C respectively of Enclosure (2).

(5) The FMSC may designate a representative on the Committee to participate as an observer. Additionally, the head of any other federal agency may request that the FMSC designate a member of their agency as an observer to the AMS Committee.

(6) Each AMS Committee shall elect one of its members as the Chairperson and one of its members as the 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. Because the AMS Committee is established and maintained under the FMSCs direction, the FMSC may chair the Committee. Nevertheless, some ports may find that, under their existing committee structure, it is more effective for industry representatives to chair the AMS Committee. Either method of chairing the AMS Committee is acceptable under the provisions of 33 CFR Part 103.

(7) The FMSC shall designate a member of his/her staff as the Executive Secretary of the AMS Committee. The Executive Secretary shall be responsible for the administrative duties of the Committee, such as maintaining current designation letters, publishing meeting agendas, recording meeting minutes, and maintaining current editions of the AMS Plan, including digital versions. It is also the responsibility of the Executive Secretary to ensure that all committee records are properly maintained and designated as Sensitive Security Information (SSI) where appropriate.

(8) 46 USCA 70112(f) states that a member of a committee established under this section, when attending meetings of the committee or when otherwise engaged in the business of the committee (including AMS Committees and the National Maritime Security Advisory Committee) is entitled to receive compensation and travel or transportation expenses. The Commandant has determined that compensation for participation on AMS Committees shall be set at zero. For travel and transportation costs, the Coast Guard has determined that a rate of $1 will apply to members of AMS Committees, as the Committees will meet locally. FMSCs may include in the Committee charter a statement that members will forego transportation, travel and compensation costs associated with participation on the AMS Committee, and all members shall sign the charter to acknowledge the waiver of travel fees and compensation. If the FMSC determines that, due to unusual circumstances, it is necessary to pay travel for a designated AMS Committee member, the FMSC may authorize travel expenses from within current operating budgets.

(9) At a minimum, 33 CFR 103.300(4) requires that AMS Committees meet at least once in a calendar year, or when requested by a majority of the AMS Committee members. Meetings need not take place in person, and FMSCs may take advantage of telephone and video conferencing when in-person meetings are impractical.

d. Sensitive Security and Classified Information.

(1) Much of the work of the AMS Committee will involve handling Sensitive Security Information (SSI). The Coast Guard's procedures for handling SSI are published in COMDTINST 5510.5, Security Classification and Designation Policy for Port Security Assessments (PSA), Critical Infrastructure (CI) Listings, and Port Security Assessment Tools (PSRAT). Policy guidance on designation and handling of SSI for the AMS Plan and AMS Committee can be found in reference (j) of this NVIC and is provided in enclosure (2). It was developed based on the rulemaking and COMDTINST 5510.5. The FMSC, in conjunction with the AMS Committee, is responsible for developing procedures to protect both SSI and classified information that is developed and used by the Committee.

(2) The handling of SSI does not require a background investigation. However, the FMSC must determine that, prior to discussing or distributing SSI with AMS Committee members, those members are "Covered Persons" with a "need to know." Guidance on "Covered Persons" and "need to know" is provided in reference (j). After being designated as a Covered Person with a "need to know," the individual receiving the SSI must sign a non-disclosure statement before the FMSC shares the SSI with the individual. A standard non-disclosure form is provided in Enclosure (2).

(3) The MSTA explicitly states in 46 USCA 70103 (d) that, "notwithstanding any other provision of law, information developed under this chapter is not required to be disclosed to the public, including - (1) facility security plans, vessel security plans, and port vulnerability assessments; and (2) other information related to security plans, procedures, or programs for vessels or facilities authorized under this chapter." Therefore, facility and vessel security plans developed under 33 CFR Parts 104, 105, and 106 for COTP zones that are under the control of the FMSC are designated as SSI, and restricted from public access. General information dealing with the port or infrastructure topics should be made available to all members of the AMS Committee with a "need to know." However, FMSCs are instructed to discuss proprietary information, and other sensitive information, such as vulnerabilities and protective strategies included in security assessments and plans, only with designated law enforcement AMS Subcommittees or select AMSC members so as to ensure proper safeguarding of the information, and to instill confidence in maritime stakeholders that sensitive information relating to their individual facilities will be afforded the utmost protection from unnecessary disclosure.

(4) AMS Committee meeting minutes and records that are not designated as SSI may be made available to the public pursuant to the Freedom of Information Act. However, FMSCs shall ensure that all material designated as SSI, and all records of discussions of material designated as SSI, are protected from disclosure to the public. Reference (j) of this circular provides additional guidance on the handling of SSI materials.

(5) It is not anticipated that AMS Committees or Plans will regularly discuss or contain information classified above the SSI level. Classified materials

incorporated into the AMS Plan should be prepared as separate documents, referenced in the unclassified plan, and handled and stored in accordance with proper security procedures. However, if the need arises to discuss information classified as Secret with members of the AMS Committee, the FMSC may request security clearances for those Committee members with whom the FMSC intends to share the information. The Coast Guard is permitted to sponsor and grant clearances for a select number of AMS Committee members. Specific procedures are found in ALCOAST 330/04 and ALCOAST 187/05.

TEMPLATE FEDERAL REGISTER NOTICE

DEPARTMENT OF HOMELAND SECURITY 4910-15-U

Coast Guard

[insert district docket number]

Area Maritime Security Advisory Committee (AMSC) [insert name of port, or other geographic qualifier]

AGENCY: Coast Guard, DHS.

ACTION: Solicitation for Membership.

SUMMARY: This notice requests individuals interested in serving on the Area Maritime Security Committee [**insert name of port**] submit their applications for membership to the COTP/FMSC [**insert name of port**].

DATES: Requests for membership should reach the U.S. Coast Guard Captain of the Port/ Federal Maritime Security Coordinator [**insert name of port**] [insert date at least 30 days after date of publication in the Federal Register].

ADDRESSES: Applications for membership should be submitted to the Captain of the Port/ Federal Maritime Security Coordinator at the following address: [**insert address]**.

FOR FURTHER INFORMATION CONTACT: For questions about submitting an application or about the AMS Committee in general, contact [**insert the name of a person with their phone number**].

SUPPLEMENTARY INFORMATION:

Authority

Section 102 of the Maritime Transportation Security Act (MTSA) of 2002 (Pub. L. 107-295) added section 70112 to Title 46 of the U.S.Code, and authorized the Secretary of the Department in which the Coast Guard is operating to establish Area Maritime Security

support of the policy of the U.S.C.G. on gender and ethnic diversity, we encourage qualified women and members of minority groups to apply.

Request for Applications:

Those seeking membership are not required to submit formal applications to the local COTP/FMSC, however, because we do have an obligation to ensure that a specific number of members have the prerequisite maritime security experience, we encourage the submission of resumes highlighting experience in the maritime and security industries.

Dated: XXXXXXXX.

I. M. Commander,
Captain, U.S. Coast Guard, Federal Maritime Security Coordinator [City]

Advisory Committees for any port area of the United States. (See 33 U.S.C. 1226; 46 U.S.C.; 33 CFR 1.05-1, 6.01; Department of Homeland Security Delegation No. 0170.1). The MTSA includes a provision exempting these AMS Committees from the Federal Advisory Committee Act (FACA), Public Law 92-436, 86 Stat. 470(5 U.S.C. App.2). The AMS Committees shall assist the Captain of the Port/ Federal Maritime Security Coordinator in the development, review, update, and exercising of the AMS Plan for their area of responsibility. Such matters may include, but are not limited to: Identifying critical port infrastructure and operations; Identifying risks (threats, vulnerabilities, and consequences); Determining mitigation strategies and implementation methods; Developing and describing the process to continually evaluate overall port security by considering consequences and vulnerabilities, how they may change over time, and what additional mitigation strategies can be applied; and Providing advice to, and assisting the Captain of the Port/ Federal Maritime Security Coordinator in developing and maintaining the Area Maritime Security Plan.

AMS Committee Membership:

Members of the AMS Committee should have at least 5 years of experience related to maritime or port security operations. The [**insert name of port**] AMSC has [**insert number**] members. We are seeking to fill [**insert number of vacancies**] with this solicitation. Applicants may be required to pass an appropriate security background check prior to appointment to the committee. Members' terms of office will be for 5 years; however, a member is eligible to serve an additional term of office. Members will not receive any salary or other compensation for their service on an AMS Committee. In

ENCLOSURE (2) TO NVIC 9-02 CHANGE 2

GUIDANCE FOR DEVELOPMENT OF
AREA MARITIME SECURITY PLANS

1. PURPOSE.

   a. This enclosure provides guidance to Federal Maritime Security Coordinators (FMSC) on the preparation and maintenance of Area Maritime Security (AMS) Plans. The AMS Committee is charged with advising the FMSC on maritime security matters, including the initial development and continual review of the AMS Plan. The Committee's input is considered vital to the planning process as the Coast Guard seeks to build on AMS Assessments to develop protection strategies, and heighten the level of security in the Nation's ports and coastal waterways.

2. BACKGROUND.

   a. The first step in developing the AMS Plan was the completion of the AMS Assessment using the Port Security Risk Assessment Tool (PSRAT), which was designed to internally assess vulnerabilities based on national security priorities. In creating its AMS Plan, each AMS Committee should have reviewed and commented upon the PSRAT, and any other relevant assessments that may have been done. Building upon those nationally focused assessments; the AMS Committee's assessment for its particular COTP zone should maintain a local emphasis and focus on priorities set by the community. Each FMSC should consider the PSRAT results when developing strategies for deploying resources within his or her zone. Future security assessments will allow for adjustments to the AMS Plan based on changing security needs and threats.

   b. The primary composition of the AMS Plan involves a tiered planning structure based on the Maritime Security (MARSEC) Threat levels. The Plans must include strategies for each MARSEC level, including pre-determined security measures to be implemented at each MARSEC Level by both Coast Guard and other members of the AMS Committee. This may include deployment of a variety of response teams that are pre-approved and triggered by changes in the MARSEC level, including Boarding Teams and Maritime Safety and Security Teams. It may also include development and implementation of regulated navigation areas, security zones, Naval Vessel Protection Zones, and U.S. Army Corps of Engineers (ACOE) restricted areas. The Ports, Waterways and Coastal Security (PWCS) Mission is an all hands evolution. No single entity has adequate resources to completely protect port areas and the associated MTS; thus, it is essential that DOD, other Federal, State and local agencies, and private industry voluntarily contribute resources to plan and implement strategies.

   c. The MTSA defines the term "facility" as any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States. This broad definition was carried forward in 33 CFR 101.105. 33 CFR Part 105 was drafted to capture and regulate under the MTSA those facilities determined by the Secretary of DHS most likely to be involved in a TSI (excluding DOD facilities). For facilities within his or her COTP zone that do not fit the description provided in Part 105, the FMSC is directed to evaluate the risks and vulnerabilities to those excluded facilities. The results of the evaluation should be reflected in the

AMS Plan. This requirement has raised many valid questions concerning the role of the FMSC in establishing protective measures for non-105 regulated facilities.

d. The MTSA does not provide COTPs the authority to impose additional requirements on vessels or facilities. Implementation of the MTSA effected a change in COTP authority only to the degree that it imposes additional enforcement authority and responsibilities on the COTP, in addition to existing marine safety and environmental protection enforcement responsibilities. If the COTP determines it necessary to impose additional requirements on vessels or facilities in his or her COTP zone, the COTPs may do so only if the authority arises pursuant to either the Magnuson Act or the PWSA, which provide that, in order to require additional security measures, the COTP must find the measures to be "necessary" in order to prevent damage. Moreover, the COTP may not issue COTP orders to require non-105 facilities to comply with portions of 33 CFR Subchapter H, or make categorical decisions about any particular type of facility, e.g., a nuclear power plant or a railroad bridge, without a specific or individual finding of necessity. The use of a COTP order without such a finding would not comply with the Administrative Procedure Act, and would likely be viewed as an illegal regulation. Accordingly, COTPs must avoid issuing orders that are not linked to specific information and findings that the orders are "necessary" to prevent damage. For example, if the Commandant raised the threat level to MARSEC Level two and the information that led to that elevation was based on a threat to bridges, it may be determined that a COTP order for security patrols on and around bridges over shipping channels is found necessary.

e. FMSCs, in collaboration with the AMS Committees, will identify security measures to be implemented in the AMS Plan. The benefit of this approach cannot be overstated. It is through the sharing of information regarding security policies and procedures, which gaps in security will best be identified and corrected. Furthermore, once identified, gaps in security should provide the basis for implementing security measures linked to MARSEC Levels. Additionally, FMSCs and the AMS Committee should coordinate with other Federal, State and local agencies that have simultaneously developed security standards for other critical infrastructure identified in the AMS Assessment. A good example is the work of the Nuclear Regulatory Commission in its development of security measures for nuclear power plants and RSPA's security regulations.

f. The final stage in the planning cycle is the training, exercising and evaluation phase. In order for a Plan to be useful, it must be practical. Each entity with assigned plan responsibilities must understand its role and how to communicate effectively with other members of the team. The evaluation and exercise phase is part of a repetitive process aimed at familiarizing participants with their roles and responsibilities, and continuously improving and updating the AMS Plan.

3. DISCUSSION

a. The AMS Plan developed by the FMSC and the AMS Committee must address the entire COTP zone, but the FMSC has discretion on how to present the geographic area covered within the Plan. This flexibility is necessary since it may be that

different geographic areas within the COTP zone have significantly disparate security concerns and protection strategies. In those cases, the FMSC may elect to complete the template provided in this enclosure for each geographic region within the zone. If the COTP chooses to compile multiple plans, the standard template and numbering system will still apply, and multiple geographic plans will be brought under the cover of a single AMS Plan. Conversely, some FMSCs may determine that certain areas within his or her COTP zone have such similar security concerns and protection strategies, e.g., Western Rivers, that he or she elects to combine different areas under one regional AMS plan.

b. The AMS Plan is a coordination tool for the port community; as such, certain sections of the Plan must remain available to all law enforcement and port agencies with port security responsibilities. Accordingly, FMSCs must remain cognizant of the methods by which SSI and other sensitive information in the Plan will be protected from unauthorized or unnecessary disclosure.

c. The AMS Plan template provided herein introduces a standard format for the development of the Plan, and is intended to assist FMSCs in ensuring that all requirements of the MTSA are addressed in their completed Plans. It builds on the template that was provided in the Navigation and Vessel Inspection Circular 9-02, Change 1, Guidelines for Area Maritime Security Committees and Area Maritime Security Plans required for U.S. Ports. Additional sections were added to the template to address the requirements of 33 CFR Subchapter H on Area Maritime Security, specifically 33 CFR 103.505. Policy guidance is provided throughout the template to assist in the development of the Plan. Bracketed text within the template indicates the information that should be provided in each section. FMSCs are allowed the unrestricted use of appendices as addendums to the Plan, which is intended to afford flexibility in its development.

d. The consistent use of the template will allow for consolidation of MARSEC strategies on a regional and national level. The standardized template will also ensure that certain sections of the Plan, for example MARSEC level 2 strategies, can easily be located in all Plans. Ultimately, the AMS Plans will be a fundamental part of the Maritime Domain Awareness Program's Maritime Common Operating Picture (MCOP).

e. The AMS Plan is primarily considered an awareness, preparedness, and prevention and recovery plan. While it does contain some response planning elements, it is not considered a response plan. Where overlaps occur with other existing crisis management plans, linkages and references should be made in the AMS Plan (AMSP) as required in 16000.27, (series). The AMSP shall also align with the National Response Plan (NRP), which is the base plan that addresses all hazards and contingencies, covering all disciplines. The NRP ensures coordination at all levels of government—Tribal, Local, State, and Federal—and cooperation with the private and public sectors in order to bring the full range of the nation's capabilities to bear in protecting the homeland. Finally, the NRP ensures that the Federal government works effectively and efficiently with State and local agencies to prevent, prepare for, respond to, and recover from domestic incidents by establishing a common National Incident Management System to be used at all levels. Areas, Districts, and

FMSCs should consult reference (s) to determine required actions and deadlines to bring the AMSP into alignment with the NRP.

f. The regulations require the AMS Committee to identify three Transportation Security Incidents (TSI) that are most likely to occur within its zone, and to develop response scenarios. The level of response planning in the AMS Plan should be very general in nature, focusing on the following three elements: 1) who has jurisdiction over the response; 2) how the command and control structure will be assembled including a determination of roles; and 3) what security resources will be brought to bear.

g. As the lead Federal Agency for maritime homeland security, the Coast Guard is responsible to accomplish the effective management and dissemination of critical security data. Accordingly, all efforts to compile security plan data in an electronic format should be made.

h. The areas of the AMS Plan that are deemed most critical are:

(1) The Area Maritime Security Committee Charter;
(2) Area Maritime Security Assessments;
(3) Communications Plan;
(4) MARSEC Levels and Implementation Directives;
(5) Control and Dissemination of Security Sensitive Information; and
(6) Preparedness for Response.

i. Best (Recommended) Practices:

(1) Terminology: Use the glossary found in the AMS Plan Template as much as possible when referring to maritime specific types of practices, equipment and people.

(2) Measurements: Use Standard English units of measurement for:

- Weight: Ounces, Pounds, Tons;
- Liquids: Ounces, Pints, Quarts, Gallons;
- Speed: Miles per hour, knots;
- Distance: Feet, Yards, Miles, Nautical Miles;
- Time: Seconds, Minutes, Hours (24 hour time system).

(3) Locations: Always include the Map/DNC Name, Series, Sheet, Number, DATUM, manufacturer and year published. If using a GPS, take the coordinate at the main entrance to the physical structure (front door of a building regardless of cardinal direction), and always state what model/make and what DATUM the GPS is using. Use only geo-coordinates in Latitude and Longitude.

(4) Data Format and Medium: Utilize standard word processing programs and, if at all possible, save and format into Adobe and PDF files. Digital and electronic formatting will simplify updating and dissemination.

(5) Photography: If photographs are used with the Plan, use digital photography or digitize (scan) standard film photographs. Save them as JPEG files to use less digital space;

(6) Imagery: If imagery is used in the AMS Plan, it is best to use ortho-rectified (direct overhead) photos. This will permit the introduction of Geographic Information System (GIS) data as overlays in the future.

AREA MARITIME SECURITY PLAN

1000 AREA MARITIME SECURITY PLAN

1100 Purpose

[No additional comments required.]

(a) The Area Maritime Security (AMS) Committee for [Blank] has created this AMS Plan. 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 MARSEC Level, complement and encompass facility and vessel security plans within its particular 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.

(c) A TSI is defined in the 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 Transportation Security Incidents (TSI). Threats and violations need to be evaluated on a case-by-case basis and responded to accordingly. It is the FMSC's responsibility to determine if and when an incident occurring in his or her zone is severe enough to warrant designation as a TSI.

1200 Captain of the Port (COTP) Letter of Promulgation

1210 Record of Changes

1300 Authority

[No additional comments required.]

(a) Section 102 of the Maritime Transportation Security Act of 2002 (MTSA), P.L. 107-295, enacted 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.

1310 Federal Maritime Security Coordinator (FMSC)

[No additional comments required.]

(a) The COTP *(List USCG unit and area/zone for this Plan)* is designated as the FMSC, charged with the responsibility of establishing an AMS Committee and developing an AMS Plan. 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.

1400 Scope

[No additional comments required.]

(a) The AMS Plan by its nature is very broad in scope, encompassing the whole of the maritime domain within a given COTP zone, and absorbing the individual assessments and planning efforts of facilities and vessels operating within that zone. The scope of each AMS Plan will be determined by evaluating the waterways, facilities, vessels, and adjacent areas that may be involved in, or affected by, a TSI in its zone.

(b) The plans required by 33 CFR Parts 104, 105 and 106 will 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, 105 and 106.

1500 Suppositions

[No additional comments required.]

(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 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, National Response Plan, and other response plans will be activated for the purpose of response and crisis management due to a TSI.

(8) All port areas are susceptible to air attack.

(9) There will be a competition for security resources as threat levels increase.

(10) *(List other assumptions, if any)*

1600 Situation

[No additional comments required.]

(a) 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. The MARSEC Levels developed by the Coast Guard are an essential tool for achieving optimum coordination, and are more fully discussed in section 3440 of this template.

1610 Physical Characteristics

(a) Describe the boundaries of the COTP zone, or Area, that the AMS Plan covers, including a:

(1) Description of identifiable bodies of water, surrounding waterfronts and significant navigable waterways in the port areas

(2) Description of the MTS infrastructure, both physical features (piers, docks, wharves) and information systems;

(3) Description of the vessel, cargo and facility interfaces and associated waterfront areas;

(4) Description of vessel traffic in the port (type and volume);

(5) Description of any secondary ports within the COTP zone;

(6) Description of port operations critical to other non-maritime related functions.

(b) Descriptions may be graphically depicted on maps and included in the Plan as appendices.

1620 Economic Characteristics

(a) Briefly describe major economic elements of the relevant COTP zone, including port activities, stadiums, national icons, large conference centers, population densities, industries, and products for the port:

(1) Types of industry:

(2) Major inter-modal connectors:

(3) Major cargos:

(4) Recent economic data:

1630 Ports, Charts and Maps

[Port charts and maps will be included in the appendices.]

2000 AREA MARITIME SECURITY COMMITTEE

2100 Introduction

[No additional comments required.]

(a) The Commandant has determined that 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 COTP/FMSC has established and convened an AMS Committee to advise the Coast Guard on maritime security matters.

2200 Purpose and Objectives

[*No additional comments required.]*

(a) The AMS Committee brings together appropriately experienced representatives from a variety of sources in its zone to continually assess security risks to the ports, determine appropriate risk mitigation strategies, and develop, revise, and implement the AMS Plans. The AMS Committees 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 COTP 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) Developing and maintaining an AMS Exercise Program.

(7) Promoting effective security measures that maintain or enhance operational efficiencies and minimize impact to legitimate trade.

(8) Advising, consulting with, and reporting to the COTP/FMSC on matters relating to maritime security.

(9) Assisting the COTP/FMSC with the communication of security information to the port and waterway stakeholders.

2300 Charter

[Insert copy of AMS Committee Official Charter here]

(a) Each AMS Committee must be established under the terms of a written charter in accordance with 33 CFR 103.300(b).

2310 Committee Structure and Procedural Rules

[This section describes AMS Committee structures and procedures. Standing procedures, such as requirement for a quorum, raising motions, record keeping, voting, terms of office, duties and responsibilities and parliamentary procedures should be documented in this section.]

(a) Each AMS Committee will elect one of its members as the Chairperson and one of its members as the Vice Chairperson. The Vice Chairperson will act as Chairperson in the absence or incapacity of the Chairperson, or in the event of a vacancy in the office of the Chairperson.

(b) The COTP/FMSC will designate a member of his/her staff as the Executive Secretary of the AMS Committee. The Executive Secretary will be responsible for the administrative duties of the Committee, such as the designation of members, publishing meeting agendas, taking of meeting

minutes, and maintaining current editions of the AMS Plan, including digital versions. The Executive Secretary is also responsible for ensuring that all committee records are properly maintained and designated as SSI as appropriate, and responsible for participation in the State, Local and Industry clearance process.

(c) Standing Committees will be designated in the charter and ad hoc committees may be developed on an as-needed basis.

(d) The AMS Committee will meet at least once in a calendar year, when requested by the COTP/FMSC, or when requested by a majority of AMS Committee members. Records of these meetings may be made available to the public upon request. However, COTP/FMSCs will ensure that all material designated as SSI will be protected from disclosure to the public.

(e) Only those members who have been determined by the COTP/FMSC to be "Covered Persons" with a "need to know" will be given AMS Committee records that contain SSI material. NVIC 10-04 provides additional guidance on the handling of SSI materials.

(f) The COTP/FMSC may nominate State, Local, and Industry members of the AMSC for a Security Clearance, sponsored by CG Headquarters (G-M). The COTP/FMSC is responsible for determining a "need to know", the assembling and forwarding of the personnel security investigation package, and all required training. Further information on this process can be found in ALCOAST 330/04 and ALCOAST 87/05.

2320 Relationship to Other Committees

(a) The AMS Committee may be related to other committees, such as:

(1) Port Readiness Committees (PRC*) [include a brief description of PRC activities/charters and their relationship to AMS Committees];*

(2) Harbor Safety Committee (HSC) [*include a brief description of HSC activities/charters and their relationship to AMS Committees];*

(3) MTS Committees [*include a brief description of MTS activities/charters and their relationship to AMS Committees];*

(4) Other committees as appropriate.

3000 AWARENESS

3100 Introduction

[Include an explanation of "maritime situational awareness."]

(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 will serve to assist the United States Department of Homeland Security (DHS) in producing a common operational picture (COP) of the maritime environment. The AMS Plan will afford critical decision makers within each COTP zone rapid access to vital information during routine and crisis maritime situations.

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

[The AMS Plan will show the jurisdictional boundaries of Federal, State, & local security and law enforcement agencies within its COTP zone. A table format is recommended with map and coordinate locations.]

(a) When depicting Federal, State and local security and law enforcement jurisdictional boundaries and areas of responsibility, first, second and third tier response agencies will be addressed separately in the AMS Plan. 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) First level agencies are those such as police, fire and emergency medical units who are normally dispatched thru the emergency 911-call system.

(2) Second level agencies are those with special 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) Third level agencies are the National Guard, military reserve, and other national level response elements.

(c) 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 COTP zone to reveal other neighboring agencies or elements that may be involved both routine and crisis situations.

3300 Area Maritime Security (AMS) Assessment

[Identify the assessment methodology information as: Who, Where, When and Results.]

(a) This AMS Plan is prepared based on an AMS Assessment, which is a risk-based analysis of the port or ports. The Coast Guard has developed a process that consists of five steps which are discussed in greater detail in Enclosure (3).

(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; and

5) Develop mitigation strategies.

3310 Maritime Security Assessment Report

[This section references the COTP zone Maritime Security Assessment, and briefly summarizes the findings in the assessment report. Suggested wording is: A maritime security assessment was conducted by_____, in January 2002 using the Coast Guard's PSRAT tool. Vulnerabilities included: _____, _____, _____, and _____. Risk reduction strategies were: _____, _____, _____, and _____.]

3400 Communications

[No additional comments required]

(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 AMS Plan must identify how and when the Committee will meet if called upon to advise and assist the COTP/FMSC in the communication of security information, what kind of assistance it will provide, and how it will provide it.

(c) The AMS Plan must also identify redundant methods for communicating vital information to ensure all appropriate facilities, vessels, maritime stakeholders, and recreational boaters are notified.

(d) The AMS Plan should address the benefits of communicating with the public, and the value of establishing programs similar to neighborhood watch programs. Programs of this nature have been found to be very beneficial in raising public awareness and involving the community in enhancing security. Further guidance is under development to assist COTP/FMSCs in developing community awareness programs that will encourage community reporting of suspicious activities and behavior.

3410 Communication of Security Information

[The AMS Committee will use the list in TAB A as a resource to identify area specific methods that can be used to ensure efficient communication of security related information.]

3410.1 Communication with the Public

[The Plan will document what means of communications will be used in emergency and non-emergency situations to communicate security

information related to the maritime environment with the general 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, and State and local emergency management offices. The AMS Committee will designate a sub-committee or working group to develop this communication process and facilitate the exchange of security information.

(b) An important element of communicating to a variety of contacts is the "community unit." The AMS Committee may designate several representatives to respond as public relations officers who are charged with developing and communicating security information to the public. These representatives should develop and maintain a comprehensive list of community leaders, emergency managers, and individuals assigned as points of contact who will implement communication protocols.

(c) COTP/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 (COTP/FMSCs) determine that exigent circumstances require communication to prevent, preempt, or disrupt an imminent threat.

(d) COMDINST 3820.14, entitled "Policy for Dissemination and Use of Intelligence Information," provides internal guidance for dissemination and use of intelligence information in support of Coast Guard objectives. It bars the COTP/FMSC from using classified intelligence as a basis for a COTP order or regulatory enforcement action (including Maritime Security Directives) without authorization from COMDT (G-M).

3410.2 Communications with Waterway Users

[The Plan will document what means of communications will be used to provide security information to waterway users in emergency and non-emergency situations and how notifications will be made.]

(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

such information. 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. TAB C identifies methods that can be used for security reports of suspicious behavior and breaches of security.

(b) America's Waterway Watch is a national awareness program that asks those who work, live, or recreate on or near the water to be aware of suspicious activity that might indicate threats to our country's homeland security. The program urges anyone who is witness to suspicious activity to report any incident to the National Response Center at 800-424-8802 or 877-24WATCH, and to report any immediate danger to life or property by calling 911. More information can be found on the program's website at http://www.uscg.mil/hq/g-m/mp/AWW_Website/

3420.1 Procedures for reporting suspicious activity

[The AMS Plan will document the procedures for reporting suspicious activity within the maritime domain.]

(a) Quick Response Cards (QRC) 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 QRC should be tailored to fit the needs of the user, but at a minimum, must include a brief introduction or instructions, ample space to collect all appropriate information, and important points of contact, incident follow up procedures, and applicable references. Several examples are provided in TAB C.

3420.2 Procedure for reporting breaches in security

[The AMS Plan will identify methods for communicating breaches in security. The AMS Assessment will determine what methods of communication are available at all MARSEC Levels and build redundancies into the system. The Plan will also document the procedures FSOs and VSOs will use to report breaches in security.]

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

State and local threat warning systems.

3410.3 Communications with Commercial Vessels

[The Plan will document what means of communication will be used to communicate security information to commercial vessels and Vessel Security Officers (VSO). This will include how the COTP/FMSC will ensure that all inbound and outbound vessels are identified at any given time, and what role the facilities and shipping agents will play in ensuring that all vessels are notified of relevant security information. The Plan will also document how receipt of security information will be verified and documented. TAB B provides a list of potential means of communication with vessels.]

(a) Communicating with commercial vessels will require a number of systems that will provide linkages to the large variety of vessels operating within the MTS. The following are examples of existing and proposed systems:

(1) Rescue 21. Rescue 21 will ensure continuous, enhanced radio coverage out to 20 nautical miles from shore. Rescue 21 is powerful enough to capture the low-powered (1-watt) marine radios transmitting from 20 nautical miles offshore. Higher-powered radios may be captured even farther offshore.

(2) The Global Maritime Distress and Safety System (GMDSS). The GMDSS is an internationally established distress and safety system, which provides automatic identification of a caller and the location of a vessel in distress.

(3) Automatic Identification System (AIS). The version of AIS required by 33 CFR Parts 26, 161, 164, and 165 automatically broadcasts vessel and voyage related information that is received by other AIS-equipped vessels and shore stations. In the ship-to-shore mode, AIS enhances maritime domain awareness and allows for the efficient exchange of vessel traffic information that previously was only available via voice communications with a Vessel Traffic Service. In the ship-to-ship mode, AIS provides essential information to other vessels, such as name, position, course, and speed that is not otherwise readily available on board vessels. In either mode, an AIS enhances mariners' situational awareness, makes possible the accurate exchange of navigational information, mitigates the risk of collision through the use of reliable passing arrangements, and facilitates vessel traffic management while simultaneously reducing voice radio telephone transmissions.

(4) Ship Security Alert System. SOLAS Regulation XI-2/6 requires certain vessels to be outfitted with a ship security alert system (SSAS), which allows the vessel to covertly signal a competent authority that the security of the ship is under threat or has been compromised.

Contracting Governments of foreign flagged vessels are required to immediately forward all SSAS transmissions from vessels within, or bound for, U.S. waters to the U.S. Coast Guard. Notification and response procedures to a SSAS alert shall be included within AMS plans. Notifications to Federal, State and local law enforcement agencies may be the primary response to a ship security alert. Field guidance on SSAS applicability, and technical guidance on the implementation of SOLAS Regulation XI-2/6, is under development.

3410.4 Communications with Facilities

[The AMS Plan shall include a list of Facility Security Officers (FSO) located within its designated area, including 24-hr contact information for each FSO. The AMS Plan will also identify what means of communications will be used to pass general and emergency security information to FSOs, including the passage of SSI. In addition, the AMS Plan will identify what means of communication will be used to verify the receipt of the passed information.]

(a) Communication of security information with regulated and non-regulated facilities within the AMS Committee's zone will be undertaken using prearranged methods that incorporate communication procedures and methods identified in individual facility security plans approved by the COTP/FMSC. The AMS Committee must design a procedure that will efficiently communicate security information pertinent to a single facility, a class of facilities, or all facilities within a geographic area.

3410.5 Communicating with Companies

[The AMS Plan will contain a list of Company Security Officers (CSO) responsible for the regulated vessels that normally operate at or within its facility, including 24-hour contact information for each officer, and will identify what means of communication will be used to pass security information to CSOs.]

3420 Security Reporting

[The AMS Plan must include measures to ensure that all individuals making reports are informed of their responsibility to contact the National Response Center and local authorities to ensure the appropriate response to a security threat.]

(a) 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 COTP/FMSC directly with

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 to ensure consistency among COTP/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 will not impose new requirements, but will 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

[The AMS Plan will include detailed procedures on the dissemination of MARSEC Directives, including who will grant access to MARSEC Directives, to whom MARSEC Directives will be issued, and a means for tracking which persons have been given access to what 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, affected entities must contact or be contacted by their local COTP/FMSC (or, if appropriate, their District Commander) to receive a copy of the MARSEC Directive. The COTP/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 COTP/FMSC through the use of a standard non-disclosure form that it will safeguard the MARSEC Directive as SSI. A standard non-disclosure form is provided in TAB D.

3430.2 Procedures for responding to MARSEC Directives

[The AMS Plan will identify procedures for receiving notice of compliance with MARSEC Directives, and for verifying that all entities affected by the MARSEC Directives are in compliance. Additionally, the Plan will

include general procedures for dealing with entities that request equivalent security measures or waivers.]

(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 COTP/FMSC or District Commander, as appropriate, and specify the methods by which the mandatory measures in the directive have been, or will be, met. In some cases, recipients may elect to submit proposed equivalent security measures to the local COTP/FMSC or District Commander, as appropriate.

3430.3 Role of the Area Maritime Security (AMS) Committee

[The Plan will identify the role of the AMS Committee in communicating MARSEC Directives.]

(a) 33 CFR 103.310 directs the AMS Committee to serve as a link for communicating threats and changes in MARSEC Levels, and disseminating appropriate security information to port stakeholders. Accordingly, the FSMC 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 AMS Committee should develop protocols and procedures addressing how it will ensure that Directives are received in a timely manner, and the means by which it will document compliance with all MARSEC Directives.

3440 MARSEC Levels

[AMS Plans must make clear the link between the MARSEC Levels and the HSAS Threat Conditions, and who sets MARSEC Level.]

(a) The Coast Guard has developed a three tiered system of MARSEC Levels consistent with the Department of Homeland Security's 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 be set commensurate with the Homeland Security Alert System (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 applies when HSAS Threat Conditions Green, Blue, and Yellow are set.

(2) MARSEC Level 2 corresponds to HSAS Threat Condition Orange.

(3) MARSEC Level 3 corresponds to HSAS Threat Condition Red.

(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 a COTP/FMSC to temporarily raise the MARSEC Level in his/her COTP 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) COTP/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 great 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 COTP/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

[Procedures for providing notification of changes in MARSEC Levels will include details, such as expected timeframes for responding to security threats and measures to ensure that vessels, facilities, and operations that are not covered by 33 CFR parts 104, 105, and 106 are informed of 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. Changes in MARSEC Levels are not considered SSI and can be disseminated by any means available.

(b) Changes in MARSEC Levels will be announced and obtained in the most expeditious means possible, preferably through a Broadcast Notice to Mariners or other existing mechanisms of communications (e.g., maritime

exchanges, VTS, VTIS programs). Whatever means used, it will be sufficient to provide timely and adequate notice to vessels and facilities regulated under 33 CFR Part 104,105, and 106.

3440.2 Notification of MARSEC Level Attainment

[Plans must provide detailed procedures for confirming compliance with changes in MARSEC Level, and the corresponding prescribed security measures. Additionally, the Plan will include general procedures for dealing with entities that cannot, or do not, comply with their security plans when a change in MARSEC Level occurs.]

(a) 33 CFR Part 104, 105, and 106 require that regulated entities confirm receipt of notice of changes in MARSEC Level, and that they have implemented the corresponding measures in accordance with their individual plans, as well as the AMS Plan. This can place a large burden on the communication systems of most COTP/FMSCs. Careful consideration should be given to determining which communication method the COTP/FMSCs will use to receive notifications, including the use of facsimile or email.

3440.3 Role of Area Maritime Security (AMS) Committee

[The AMS Plan will include details of how AMS Committee members shall assist in communicating changes in MARSEC Levels.]

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 NVIC 10-04. 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, or other applicable law and regulations.]

3600 Maritime Security Training

(a) Each member of the AMS Committee is responsible for ensuring that those members of their Committee directly affected by the execution of the AMS Plan are sufficiently trained to execute their roles in implementing the AMS Plan.

3700 Security Resources

[The AMS Plan will include a section that lists all of the security resources that are available for incident response and what their estimated timeframe is for the dispatch of responding units.]

4000 PREVENTION

4100 Introduction

(a) The COTP/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

4220 Procedures to Be Used When a Vessel and a Facility Are At Different MARSEC Levels:

[The AMS Plan will identify the COTP/FMSC procedures to ensure an inbound vessel is instructed to raise its MARSEC Level, and will describe what notifications are required to both vessels and the COTP/FMSCs when a facility receives information that a vessels is arriving operating at a lower MARSEC Level than the facility. The AMS Plan will also describe the corrective action that must be taken in that instance.]

(a) When a vessel is operating at a higher MARSEC Level (as defined by the ISPS Code) than the facility or port which is its destination, (e.g., when it has been directed to a higher level by its flag state or at the discretion of the vessel owner), the port and its facilities may remain at their existing MARSEC Level. However, if the port or facility is at a higher MARSEC Level than the arriving vessel per Commandant or COTP/FMSC direction, the vessel must attain the corresponding MARSEC Level as directed by the AMS Plan or the COTP/FMSC.

4230 Procedures for Requesting Equivalencies and Waivers to MARSEC Directives

[Describe procedures for requesting equivalencies and waivers for specific measures required by the MARSEC Level. Explain how the COTP/FMSC will convey approval of equivalencies.]

(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 COTP/FMSC receipt of the MARSEC Directive, as well as specify the method by which the mandatory measures have been (or will be) met. Pursuant to 33 CFR 101.130, owners or operators may propose to the local COTP/FMSC equivalent security measures that have been approved by Commandant (G-MP) as meeting or exceeding the effectiveness of the required measure.

(b) In addition, 33 CFR §§ 104.130, 105.130, and 106.125 state that vessel or facility owners or operators may request waivers for any requirement of Parts 104, 105, or 106 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.

4300 MARSEC Level 1

4310 Roles, Resources, Authorities, and Responsibilities

[Describe how, and by whom, security procedures will be implemented.]

4320 Standard Security Procedures for MARSEC Level 1

[The AMS Plan will specify the COTP/FMSC review process for MARSEC Level 1 requirements in current Area OPLAN and/or OPORD and EXORD.]

4330 Physical Security Measures

The AMS Plan will consider the following physical security measures where appropriate for vessels and facilities, and vessels and facilities not regulated under 33 CFR Parts 104, 105, or 106:

(a) Planning for and establishing Fixed Security Zones and Regulated Navigation Areas (RNAs), and specifying who is going to enforce them;

(b) Incorporating security elements into the duties and responsibilities of all port personnel:

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

(c) Establishing restricted areas to control access:

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

(2) Mark restricted areas;

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

(4) 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;

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

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

(d) Procedures for notifying vessels and facilities in the COTP zone that MARSEC Levels 1 has been set;

(e) Designating areas where control measures shall be implemented;

(f) Denying access to anyone refusing to submit to security verification;

(g) Monitoring the port, including during the hours of darkness and other times of poor or restricted visibility;

(h) Establishing procedures and means of communicating any threatening acts;

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

(j) Offering to review physical security plans and procedures for facilities not regulated under 33 CFR 105 or 106, 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.

4340 Operational Security (OPSEC) Measures

(a) Operational Security is defined as a systematic and analytical process by which the U.S. Government and its supporting contractors can deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of planning and execution of sensitive activities and operations.

(b) The information about Coast Guard 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 personnel, including active duty, reserve, auxiliary, civilian and contractors. A concerted effort must be made to ensure that all personnel are aware that the threat is real and active in all aspects of Coast Guard missions.

(c) COMDTINST M5510.23 outlines OPSEC planning and implementation in detail.

4400 MARSEC Level 2

4410 Standard Security Procedures for MARSEC Level 2

[The AMS Plan will specify the COTP/FMSC review process for MARSEC Level 2 requirements in current Area OPLAN and/or OPORD and EXORD.]

4420 Roles, Resources, Authorities, and Responsibilities

[Describe how, and by whom, security procedures will be implemented.]

4430 Physical Security Measures

(a) The AMS Plan shall consider the following physical security measures where appropriate for vessels and facilities, and vessels and facilities not regulated under 33 CFR Parts 104, 105 or106:

(1) Enhancement of security procedures identified for MARSEC Level 1;

(2) Review of security roles and responsibilities;

(3) Controlling access to restricted areas to allow only authorized personnel;

(4) Inclusion of 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) Giving consideration to requiring additional security measures for facilities not regulated under 33 CFR 105 or 106, 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 Operational Security Measures

[The AMS Plan shall detail procedures to verify attainment of MARSEC Level 2 OPSEC measures, and may give consideration to requiring additional OPSEC measures for safeguarding information related to vessel arrivals, departure, shiftngs, and cargoes. Within four hours of receiving reports of MARSEC 2 attainment, COTP/FMSCs will conduct spot checks of OPSEC measures employed by vessels and facilities, and vessels and facilities not regulated under 33 CFR parts 104, 105, and 106, and immediately advise

owners/operators of any concerns.]

4500 MARSEC Level 3

4510 Standard Security Procedures for MARSEC Level 3

[The AMS Plan will specify the COTP/FMSC review process for MARSEC Level 3 requirements in current Area OPLAN and/or OPORD and EXORD.]

4520 Roles, Resources, Authorities, and Responsibilities

[Describe how, and by whom, security procedures will be implemented.]

4530 Physical Security Measures

[The AMS Plan shall consider the following physical security measures where appropriate for vessels, facilities, and vessels or facilities not regulated in 33 CFR parts 104, 105 or 106.]

(a) Continuation and enhancement of security procedures required at MARSEC Level 1 and 2;

(b) Identification and employment of mechanisms to ensure that regulated vessels and facilities:

(1) 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;

(2) 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;

(3) Protect against an imminent security incident, e.g., inspect all persons, personal effects and vehicles.

(c) Giving consideration to requiring additional security measures for facilities not regulated under 33 CFR 105 or 106, 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.

4540 Operational Security Measures

[The AMS Plan will require verification of MARSEC Level 3 OPSEC measures, and may give consideration to requiring additional OPSEC measures for safeguarding information related to vessel arrivals, departures, shiftings and cargoes. Within one hour of receiving reports of MARSEC Level 3 attainment, the COTP/FMSC will begin checks of OPSEC measures

employed by vessels, and facilities, and vessels and facilities not regulated under 33 CFR 104, 105 and 106, and immediately advise the owner/operator of any violations.]

4600 Public Access Facility

[The purpose of this guidance is to provide instruction for COTP/FMSCs and facility owner or operators regarding application, review, and granting Public Access Facility (PAF) exemptions per 33 CFR 105.110(d). Designation of a PAF does not constitute total exemption of 33 CFR Part 105. To ensure national consistency, COTP/FMSCs shall incorporate this guidance when considering exemption requests.]

4610 Designation of Public Access Facilities (PAF)

[The Plan will list (1) all designated Public Access Facilities (PAF) within the area; (2) the security measures that must be implemented at the Public Access Facility at various MARSEC Levels; and (3) who is responsible for implementing the measures and how to contact them, Including 24-hour contact information.]

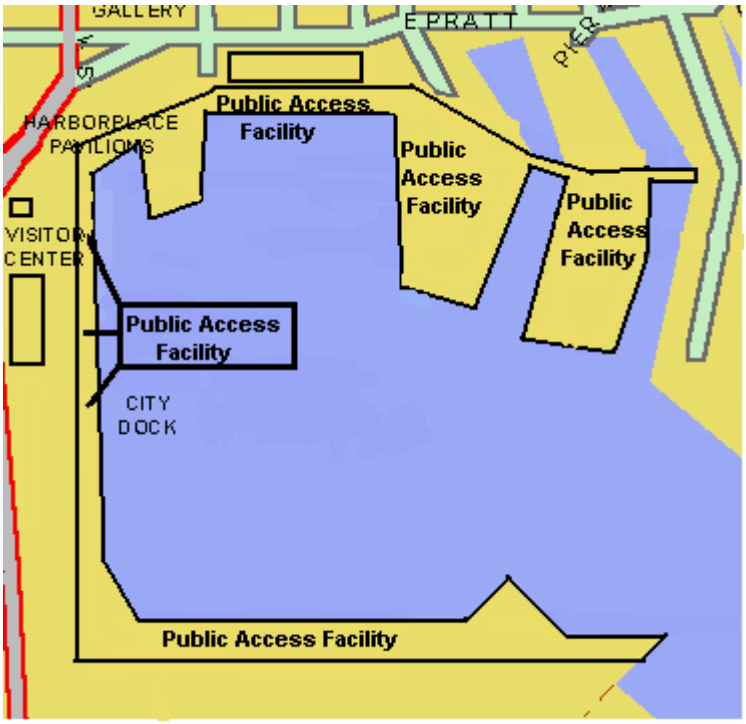
(a) An owner or operator of a facility seeking exemption of 33 CFR 105 may request to the cognizant COTP/FMSC, designation as a Public Access Facility (PAF). As per 33 CFR 101.105, the definition of a PAF is an area with public access that is primarily used for recreation or entertainment purposes, and 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 minimal infrastructure, such as only bollards, cleats, or ticket booths. Tab E has been developed to aid in determining PAF exemption applicability. Tab F provides a sample exemption request letter.

(b) Before granting the exemption, the COTP/FMSC shall consider the results of the AMS Assessment. The COTP/FMSC will notify the facility in writing whether its request for designation as a PAF has been approved or disapproved.

(c) If the designation is granted, the facility is not relieved from all security responsibilities, and may be required by the COTP/FMSC to implement specific security measures as a condition of the designation. The COTP/FMSC may also require a written agreement from the owner or operator of the PAF indicating that adequate security will be provided at the facility during periods of heightened MARSEC Levels. For example, the COTP/FMSC may consider requiring the facility owner or operator to provide additional guards to monitor the PAF at MARSEC Levels 2 or 3, or during special events. This written agreement does not limit the COTP/FMSC's authority to require the implementation of additional security measure to deal with specific security concerns as they arise.

(d) Figure 1 is an example of how the boundaries of a Public Access Facility could be designated. Typically, the perimeter has no physical barriers, allowing unimpeded access to the facility.

Figure 1. Public Access Facility



4620 Review and Evaluation of Request

(a) The COTP/FMSC shall conduct a complete review and evaluation of the PAF exemption request. This review and evaluation should also consider the results and impacts related to the AMS Assessment.

(b) To assist the COTP/FMSC with considering this request, an on-site evaluation may be necessary to verify PAF exemption applicability.

4630 Establishment of Conditions

(a) Once PAF exemption applicability has been determined, the COTP/FMSC should coordinate with the owner or operator of the facility to establish conditions for which this exemption is granted. Tab G provides required and additional security measures the COTP/FMSC may impose. To ensure consistency the additional security measures should be limited to those listed in the “Additional Requirements to Review for Applicability” column.

(b) Tab G was developed considering the existing Facility Security regulations. The tool provides required and recommended security measures. The “Required Measures” are the minimal security measures applicable to all

PAFs. The "Additional Requirements to Review for Applicability" listed in the tool must be considered and shall be implemented as necessary based on COTP port assessments.

4640 Issuance of Designation Letter

(a) After a complete evaluation of the facility has been conducted and security conditions have been established, the COTP/FMSC shall issue a PAF Designation Letter. Tab H provides a sample designation letter. At a minimum the designation letter shall include a list of established security conditions that shall be implemented at the PAF. Security conditions shall be included as an enclosure to the designation letter and considered SSI. See Section 3500 of this NVIC for further guidance on the handling of SSI. The PAF owner/operator shall acknowledge and accept these conditions in writing.

(b) A copy of the designation letter and acknowledgement shall be kept on file with the AMS Plan for as long as the designation is valid.

(c) Appropriate MISLE entries, including Facility Identification Number and 24-hour contact number of the individual with security responsibilities shall be completed.

Note: PAFs should be designated in MISLE as a "MTSA Facility – No Plan Required".

4650 Vessel Responsibilities When Calling at a PAF

(a) General Responsibilities

(1) The Vessel Security Plan must address security concerns while at the PAF, per 33 CFR 104.292(d).

(2) The vessel is responsible for implementing all appropriate security measures while at the PAF, however, they may liaison with the PAF to determine who will actually perform security activities.

(3) At MARSEC 1, 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 Area Maritime Security Plan includes a list of PAFs, their designated Individuals with Security Responsibilities and COTP/FMSC requirements.

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

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

(6) At MARSEC 2, 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 determine security measures that will be in place at the PAF.

(7) 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.

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

(9) At MARSEC 3, 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 determine security measures that will be in place at the PAF.

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

4660 Compliance

(a) Facilities, operating under an approved FSP, that wish to be considered for designation as a PAF must submit a request to the COTP/FMSC at least 60 days prior to the requested designation date.

(b) Facilities not in operation that wish to be considered for designation as a PAF must submit a request for Designation as a Public Access Facility to the COTP/FMSC no later than 60 days prior to beginning operations.

(c) Facilities requesting designation as a PAF must comply with the Facility Security Plan submission requirements in 33 CFR 105.410(b) {i.e. 60 days prior to beginning operations} until such time as the PAF designation is granted.

(d) If a facility has a change in ownership, the Individual with Security Responsibilities must submit updated contact information to the COTP/FMSC. The owner/operator of the PAF shall conduct a review of the PAF designation and conditions and notify the COTP/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

(e) After receiving the request, the COTP/FMSC will either:

(1) Approve it with conditions via PAF Designation Letter.
(2) Request additional information to make a determination.
(3) Disapprove it, with a letter restating requirements under 33 CFR 105 (or stating facility does not meet requirements of 33 CFR 105).

(f) The PAF designation and COTP/FMSC conditions will be evaluated annually to ensure the exemption remains appropriate. Any changes to the operations or description of the facility must be immediately reported to the COTP/FMSC.

4670 Enforcement Actions

[*Do not include specific enforcement actions in the AMS Plan, include only a general discussion that enforcement actions will be taken when COTP/FMSC deems necessary.]*

(a) Three anticipated types of non-compliance:

(1) Incorrect contact information for Individual with Security Responsibilities.
(2) PAF will only be temporarily out of compliance with COTP/FMSC Conditions.
(3) Permanent or frequent non-compliance.

(b) Possible enforcement actions:

(1) Informal request for immediate correction/update for administrative discrepancies.
(2) COTP/FMSC letter request for correction/update within a specified/reasonable timeframe.
(3) COTP/FMSC Order suspending operations with vessels regulated under 33 CFR Part 104 until in compliance.
(4) Consider civil penalty action.
(5) Revoke their designation as PAF, require full compliance with 33 CFR Part 105, and consider issuing a COTP/FMSC Order with conditions under which they will be allowed to operate until their FSP is approved.

Note: 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.

4700 Maritime Worker Credentials (reserved)

5000 PREPAREDNESS FOR RESPONSE

5100 Introduction

[Preparedness for response in the context of this section is primarily designed to provide post-incident consequence mitigation linkages. Port/Area contingency response plans do not need to be repeated here, but will require a reference.]

(a) The supposition for developing a post-incident segment of the AMS Plan is that an incident has occurred. This section will provide the information necessary to identify the following:

(1) Who will respond to the specific security incidents;

(2) What resources responders will bring with them;

(3) The incident command structure; and

(4) The communications required to mitigate the impact of a TSI.

5110 Procedures for responding to suspicious activity.

[This section will include the response procedures to be implemented in the event of a report of suspicious activity within a particular COTP/FMSC AOR.]

5120 Procedures for responding to breaches of security.

[This section will identify what entities are responsible for responding to breaches of security. The AMS Committee shall consider geographic capabilities of Federal, State, County, and local law enforcement entities and consequence mitigation resources in determining which entities will respond to breaches of security at high consequence targets.]

(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."

5200 Transportation Security Incident (TSI)

5210 Procedures for Notification

[Specific notification procedures must be described in this section.]

(a) 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 COTP/FMSC or their representative, then to the NRC.

5220 Incident Command Activation

[The AMS Plan will address the steps necessary to activate a crisis management command operations center.]

(a) The COTP/FMSC, normally in consultation with partner agencies, will determine whether there is a need to establish an incident command or unified command for a particular incident, and that its structure follows the guidance in the National Response Plan.

5230 Threats That Do Not Rise to the Level of a TSI.

(a) 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. Incidents that reveal serious discrepancies or weaknesses within required plans will be reported to the COTP/FMSC.

5300 Most Probable Transportation Security Incident

[This section will describe the types of TSIs most likely to occur in the AMS zone, and the procedures and steps that will be taken to respond.]

(a) Because each port area has unique characteristics, different types of TSIs are likely to occur more frequently in one port area than another. COTP/FMSCs should use the results of the AMS Assessment to identify the three types of TSIs most likely to occur within his or her zone.

(b) Since it is impossible to plan for every scenario, COTP/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. Plans should also focus on several types of scenarios to ensure most port stakeholders are involved in planning efforts. Accordingly, there should be at least one scenario involving a vessel, one for a waterfront facility, and one for a common infrastructure, such as a bridge, tunnel, dam, lock, or other significant structure.

(d)Since the AMS Plan is not a response plan, but an awareness, preparedness and prevention plan, scenario development should consider possible roles, responsibilities, and resources very broadly and be limited to determining who will respond, what their roles will be, and what resources they can provide. For the initial AMS Plan submission, it is not envisioned that this section will require the level of detail necessary in drafting an Incident Action Plan.

5310 Identify Command Structure with Assigned Roles (ICS Flowchart)

[For each of the three required scenarios, the AMS Plan will include an Incident Command System flow chart identifying the assigned roles of the primary responders to the incident.]

5320 Procedure for Responding To TSI

[For each of the three required scenarios, identify the jurisdiction of those responding and what resources they will provide.]

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

[For each of the three required scenarios, identify what other relevant Federal, State and local plans may be implemented as a result of the scenario.]

6000 CRISIS MANAGEMENT AND RECOVERY

6100 Introduction

[Each transportation system within the COTP zone must be prioritized from most to least essential according to its importance to the continuity of operations of the port or zone.]

(a)Normally, post-incident recovery of the MTS after a TSI will be coordinated through the COTP/FMSC, other government agencies, and relevant portions of the private sector.

(b)General priorities for recovery are:

(1) Major transportation routes needed for emergency services, including evacuation 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 out-loads;

(4) Secondary bridges and tunnels;

(5) Main shipping channels critical to major commercial operations;

(6) Secondary commercial waterways;

(7) Public/recreational waterways.

6200 Procedures to Maintain Infrastructure

[The AMS Plan will prioritize infrastructures according to their importance in maintaining the continuity of operations of the port and the procedures for maintaining infrastructure integrity.]

6300 Procedures for Recovery of MTS

[The AMS Plan will prioritize the procedures for most efficient recovery of the MTS and for reopening port(s), and affected waterways, or provide linkages to port plans that address recovery of the MTS.]

7000 COMPLIANCE MEASURES

(a) The MTSA regulations rely on existing COTP authority to implement compliance measures. The control and compliance measures contained in 33 CFR 101.410 provide the FMSC with a large degree of flexibility in rectifying non-compliance of vessels and facilities regulated under 33 CFR part 104, 105, and 106. Guidance on using control measures is contained in the Marine Safety Manual (MSM), Volume I, Chapter 4, and should be considered in determining appropriate compliance measures. In some cases, a violation may carry both civil and criminal penalties. In cases where evidence exists that a major violation has occurred, the matter will be referred to the District Commander in accordance with MSM Vol. I, 4.D.2.d.

8000 AREA MARITIME SECURITY PLAN AND ASSESSMEMT SYSTEM MAINTENANCE

(a) The goal of this section is to clearly establish baseline procedures and timelines for the regular review, amendments, and approval of AMS Assessments and AMS Plans. It is important to understand that the following procedures are the minimum standards for the maintenance of the AMS Plans and AMS Assessments. COTP/FMSCs are encouraged to establish additional procedures to ensure that there is a robust review program to maintain a desired level of preparedness.

8100 Procedures for the Regular Review and Maintenance of the AMS Assessments

(a) Quinquennial Area Maritime Security Assessment (Five Year Cycle):
Every 5 years AMS Committee shall conduct a formal risk based assessment for the entire area over which it has responsibility. This assessment shall be completed with sufficient time to ensure that any changes prompted by the assessment is addressed in the quinquennial submission of the AMS plan.

(b) Annual Validation of the existing Area Maritime Security Assessment: Current AMS assessments shall be evaluated at least annually to review their adequacy, feasibility, consistency, and completeness to identify gaps in security. Annual reviews should be completed prior to an AMS exercise. Changes or adjustments to the assessments do not require formal review by the Districts or Areas Commanders. However, COTP/FMSCs must inform their respective chain of commands when significant changes do occur.

(c) Immediate Changes to the Area Maritime Security Assessment: There may be occasions for an immediate change to an assessment. For example, new threat products or intelligence may cause an aspect of the port infrastructure to be a known target. In those circumstances COTP/FMSCs should follow the same procedures as for the annual validation noted in section (b) above.

8200 Procedures for the Regular Review and Maintenance of the AMS Plans

8210 Quinquennial Review and Approval of AMS Plans (Five Year Cycle)

(a) Every 5 years AMS Committees shall conduct a detailed review of the AMS plan. The Area Commander is responsible for managing the schedule of the five year review cycle and ensuring that the five year review and approvals are conducted. Area Commanders will set and post the schedule for the Quinquennial review process in order to distribute the review and approval workload evenly. This formal review should focus on the results of the Quinquennial Area Maritime Security Assessment and how the findings of the assessment affect the AMS plans. In particular they should account for changes in port infrastructure and critical port operations. Once the AMS Plan has been reviewed by the AMSC, the AMSC chairman will inform the COTP/FMSC of its recommendations to change the plan in accordance with findings from the assessments. Once the AMS Plan amendments are made, the COTP/FMSC will ensure that the amended plan is forwarded to the cognizant District Commander.

(b) Upon receipt of a revised or updated plan, the District Commander will review the AMS plan. If the District Commander recommends changes or amendments to the plan as a result of his/her review, the District Commander will coordinate with the cognizant COTP/FMSC to ensure that any required changes or amendments are completed. The District Commander will review the plan, then forward to the Area Commander for review and final approval.

(c) If the Area Commander recommends changes or amendments to the plan as a result of his/her review, the Area Commander will coordinate with the District Commander to ensure that the cognizant COTP/FMSC makes the required changes or amendments. Once the Area Commander has

approved the plan submitted for the five year formal review, he/she will notify the Assistant Commandant for Marine Safety, Security and Environmental Protection.

8220 Annual Validation of the Area Maritime Security Plans:

(a) AMS plans shall be evaluated at least annually for adequacy, feasibility, consistency, completeness and to identify gaps in security. Annual reviews should be completed prior to the conduct of an AMS exercise. Changes or adjustments to the plans do not require formal review by the Districts or Areas. However, COTP/FMSCs must inform their respective chains of commands when significant changes do occur.

8230 Immediate Changes of the Area Maritime Security Plans:

(a) There may be occasions for immediate changes to the plans. The following are some examples of information that would warrant immediate changes:
   (1) Change or 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 physical changes that alter avenues of access to port.

(b) For immediate changes to plans COTP/FMSCs should follow the same procedures as for the annual validation as noted in section (b) above.

9000 APPENDICES (OPTIONAL)

(a) 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. As such, some information contained in the Plan is better suited for inclusion in an appendix due to the size or sensitive nature of the information. For example, some information, although not SSI, would be exempt from public disclosure pursuant to 5 USC 553(b).

(b) Examples of appendices are listed below. With the exception of the glossary, the appendices are optional for the development of the AMS Plan.

9100 Area Maritime Security (AMS) Committee Members

[Insert any information tables containing contact and agency names, phone numbers, email addresses, and/or other specific information pertaining to Committee members.]

(a) Due to the nature of the information contained in this appendix, some may be exempt from public disclosure pursuant to 5 USC 553.

(a) Due to the nature of the information in the AMS Assessment, this appendix will be classified SSI and maintained separately from the AMS Plan in accordance with 49 CFR Part 1520.

9400 Risk-Based Scenarios

[Insert results of the risk-based AMS Assessment pertaining to the identification of threat scenarios specific to a given COTP zone]

(a) Due to the nature of the information in the AMS Assessment, this appendix will be classified SSI and maintained protected from release in accordance with 49 CFR Part 1520.

9500 Dangerous Cargos for Security Planning

9600 Glossary of Terms

(a) A glossary of terms, developed by the Coast Guard Maritime Homeland Security Integration Team, is provided on G-MP intranet site at http://cgweb.comdt.uscg.mil/g-mp/docs/pdf/PWCS_SDP_AppA_30Sep03.pdf . It was originally developed as an appendix to the Ports, Waterways and Coastal Security (PWCS) Strategy Deployment Plan. The AMS Plan will use the standard terms identified in this glossary.

Tab Index

TAB A

U.S. Department of Homeland Security

United States Coast Guard

Command
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-
Phone: (202) 267
Fax: (202) 267
Email:

16601

Dear_____:

It is a great pleasure to invite you to serve as a member on the Area Maritime Security (AMS) Committee *[or Executive Steering Committee, or relevant committee]* for *[insert name of AMS Committee or other committee as appropriate, e.g., USCG 8th District]*. You were chosen based upon your skills, experience and expertise in the maritime field, and the vital service your participation will contribute to the safety and security of the Nation's ports and waterways.

Although I hope you will consider it an honor to be chosen, the appointment will demand a significant commitment of your time. Furthermore, this appointment is not funded and, therefore, you will receive no monetary compensation for your participation. Before accepting, I encourage you to review the Code of Federal Regulations, Title 33, Part 103, particularly Sections 300, 305, and 310, which describe the establishment, composition and responsibilities of all AMS Committees, and which will provide the foundation for the *[name of Committee]* upon which you will serve if you accept the appointment.

By accepting the appointment, you will be committing to abide by the rules in Title 33 of the Code of Federal Regulations, Parts 101 and 103, by the Committee's charter, and to act in good faith and to the best of your abilities in the application of the policies and procedures established by the *[name of the Committee]*. If you choose to accept this invitation, your appointment to the _____ Committee will be for *[# of years]*.

To accept this appointment, please complete and return to me at your earliest convenience *[or some specific period of time]* the enclosed Acceptance of Appointment letter with your signature indicating that you understand and accept your commitment and responsibilities as a member of the *[Name]* AMS Committee. Upon receipt of your acceptance letter, you will be sent a Letter of Appointment and further information regarding your future participation.

I look forward to hearing from you and serving with you on the AMS Committee in the immediate future.

Sincerely,

_____
Captain, U.S. Coast Guard
Federal Maritime Security Coordinator

Enclosure: Acceptance of Appointment Letter

Copy: _____ Committee
Commander, _____Coast Guard District (m)

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

Command
United States Coast Guard

2100 Second Street, S.W.
Washington, DC 20593-0001
Staff Symbol: G-
Phone: (202) 267
Fax: (202) 267
Email:

16601

Letter of Appointment to the _____ AMS Committee

Dear _____

It is my pleasure to appoint you as a member of the Area Maritime Security (AMS) Committee *[or Executive Steering Committee, or relevant committee]* for *[insert name of AMS Committee or other committee as appropriate]*. This appointment is effective *[insert date]* and shall expire on *[insert date]*.

I have enclosed a copy of the *[name, e.g., USCG 8th District]* AMS Committee Charter. It describes in detail the Committee's purpose, membership rules, and other important information essential to your service on the Committee. Please contact _____ of my staff at your earliest convenience regarding the upcoming schedule of *[AMS/Executive Subcommittee]* meetings.

Thank you for your service to your community and the Nation. I look forward to seeing you at our next Committee meeting.

Sincerely,

_____
Captain, U.S. Coast Guard
Federal Maritime Security Coordinator

Enclosure: Committee Charter

Copy: _____ Committee Chair
Commander, _____ Coast Guard District (m)

Acceptance of Appointment

to the

_____Committee

I hereby accept an appointment to serve on the _____ Committee, for a period to be designated by the Federal Maritime Security Coordinator, and pledge to be bound by the Code of Federal Regulations, Title 33, Parts 101 and 103, and the _____ Committee Charter, and to act in good faith and to the best of my abilities in the application of the policies and procedures established by the _____ Committee in accordance with all applicable laws and regulations.

I understand that I am not authorized to deputize others to attend meetings in my place. I further understand that the Federal Maritime Security Coordinator may revoke my appointment at any time he or she determines it is necessary for the efficient and effective functioning of the Committee. By signing below, I further acknowledge that I will not be entitled to any compensation or reimbursement of expenses connected with my participation on the _____ Committee.

This ___ day of _____, 20__.

_____

[Appointee's Name]

Communicating Security Information (Facilities)

Method	Pro's	Con's	Type of info that it can be effective for
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)	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	
Port Security Facility Officer under ISPS Code (MTSA designated USCG COTP as this)			
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 (i.e. pilots to VTS)	Not used everywhere Requires training and awareness Security could be compromised	

Communicating Security Information (Commercial Vessels)

Method	Pro's	Con's	Type of info that it can be effective for
GMDSS			
NAVTEX	Very regional, so can provide specific info	Deep-sea only 1-way comms only (vessel receives info, but can't send) Cannot be used for SSI info	Communicating info to ships entering US waters
E-mail	Mass distribution Reliable Handles lots of info 2-way comms	Have to have a computer 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)
AMVER	Provides world-wide geographic position of vessels Can be used 2-way	Normally 1-way comms only (vessel to system) Voluntary	Can be used to identify position of ships Can be used to provide ANOA's
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	Widely available Immediately available 2-way Economical	Short range – line of sight, although repeaters can be used Not secure Not 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	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 (will operate)	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	Widely available Inexpensive	Limited range Not reliable Not secure System prone to overload Can't be used for mass communications (conf. Calls)	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
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

SUSPICIOUS ACTIVITY

COMMENTS: This Action Plan is for use in a situation not covered by another QRC and in situations involving reports of negligent or unlawful behavior on the part of mariners, industry, or members of the community.

INITIAL INFORMATION Date/Time of Report_____
OOD_____

Reporting Party_____
Phone_____

Location_____
___

VESSEL INFORMATION:

Vessel_____ Vessel Type_____

Lloyds Number_____
Homeport_____

Gross Tons_____ Deadweight Tons_____ Prop Type_____

Cargo Type_____
Amount_____

Lat_____ Long_____
Course/Speed_____

Port of Origin_____ Destination_____
ETA_____

Owner_____
Phone_____

Agent _____ Phone_____
Fax_____

Other information_____

_____
____

FACILITY INFORMATION:

Facility_____
Location_____

POC_____

Phone_____

Other
information_____

_____
____

OTHER INFORMATION:

Agencies on scene_____ USCG resources on
scene_____

DESCRIPTION OF SITUATION:
_____

_____
____

_____
____

SUSPICIOUS ACTIVITY (cont)

ACTION CHECKLIST		YES	NO	TIME/DATE	OTHER
Arrange:	FOSC	___	___	_____	_____
	Firefighting	___	___	_____	_____
Underway:	Boat	___	___	_____	_____
	Helo	___	___	_____	_____
Dispatch/	Recall Team	___	___	_____	_____
Notify:	MER	___	___	_____	_____
	Port Safety	___	___	_____	_____
	Duty Inspector	___	___	_____	_____
	Duty Invest.	___	___	_____	_____
	MSD	___	___	_____	
Establish	Safety Zone	___	___	_____	_____
	Security Zone	___	___	_____	_____
	COTP Order	___	___	_____	_____
	Custom's Hold	___	___	_____	_____
	Restricted Airspace	___	___	_____	_____
Notify:	CDO /CPOPS/XO/CO	___	___	_____	_____
	VTS	___	___	_____	_____
	District	___	___	_____	_____
	GROUP OPCEN	___	___	_____	_____

	MSD	___	___	_____	_____
	Sheriff	___	___	_____	_____
	Police	___	___	_____	_____
	U.S. Marshal	___	___	_____	_____
	FBI	___	___	_____	_____
Messages:	SITREP/POLREP	___	___	_____	_____
	BNTM	___	___	_____	_____
	Req. Resources	___	___	_____	_____
Case Info:	Statements	___	___	_____	_____
	Photos	___	___	_____	_____

Other action taken_____
_____
_____

TERRORISM/HOSTAGE SITUATION

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

INITIAL INFORMATION Date/Time of Report_____
OOD_____

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 on scene:

Communications:

Other
Comments_____

_____

_____

TERRORISM/HOSTAGE SITUATION (cont.)

ACTION CHECKLIST
(Time) (Person Notified)

____ Notify CDO
____ Notify District Command Center _____
____ Notify State and Local Enforcement Agencies
_____
____ Notify FBI (###)-###-#### _____
____ 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.
____ Notify VTS when applicable

ADDITIONAL REFERENCES:
a. Marine Safety Manual, Vol. X, COMDTINST M16000.15 (page 79-21

BOMB THREAT - Vessel or Facility

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 of 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. Sector _____ 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 <u>Don't Hang Up!!</u>

INITIAL INFORMATION Date/Time of Report_____
OOD_____

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_____

QUESTIONS TO ASK

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)

DESCRIPTION OF CALLER'S VOICE

Male/Female_____ Age_____

Intoxicated_____ Speech Impediment_____
Accent_____

Scripted_____ Ad Lib_____
Recorded_____

BACKGROUND NOISES:

Music_____ Children_____
Airplane_____

Talk_____ Traffic_____
Typing_____

Machines_____ Boating_____
Fan/Vent_____ Other_____

BOMB THREAT - Vessel/Facility(cont.)

ACTION CHECKLIST
(Time)

____ 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 CDO
____ Notify State Police Bomb Squad (###) ###-#### _____
____ Notify FBI (###) ###-#### _____
____ Notify Police Dept. and Fire Dept. via 911
_____
____ Notify VTS (Consider waterway and traffic issues) _____
____ Notify District Command Center _____
____ Find what assistance, if any, are the Police requesting from the USCG
____ Determine if emergency Safety Zone is necessary.
____ Determine if small boat assistance in transporting Bomb Squads to vessel (CG Asset) is necessary.
____ Determine is small boat assistance in evacuating personnel (CG Group) is necessary.

ADDITIONAL REFERENCES:
(a) 33 CFR 6.19
(b) Marine Safety Manual, Vol. VII (Chapter 6)
(c) CGD_ SOP
(d) Physical Security Manual, COMDTINST M5530.1

DEFINITION OF PUBLIC ACCESS FACILITY

1. In order to be considered a Public Access Facility, the Facility must fall under the requirements of 33 CFR 105.105 (a)(2).

A facility that falls under any other paragraph of the 105 applicability would not be able to meet the definition of a Public Access Facility because those facilities would handle cargo. According to the comments section of the Federal Register, "We have not allowed public access facilities to be designated if they receive vessels such as cargo vessels because such cargo-handling operations require additional security measures."

2. In order to be considered a Public Access Facility, the facility must meet the definition outlined in Part 101.105.

Under the Public Access Facility definition, there are 3 paragraphs. A facility must meet all 3 paragraphs to meet the definition.

3. 33 CFR 101.105, definition of Public Access Facility, Paragraph (1) talks about a facility being used "primarily for purposes such as recreation, entertainment, retail, or tourism."

Does this apply to a commuter ferry dock or landing, which receives vessels that carry passengers and may also be used for recreation purposes, such as people fishing off the dock? Yes, if the Public has access to the dock, they may use the dock at any time for recreation, therefore the ferry does not have exclusive use of the dock. The dock is multi-use, has public access, minimal infrastructure, and there does not seem to be a need to apply all of 105 to this dock. The sentence says "such as", so the four purposes listed are examples, and are not all-inclusive.

4. 33 CFR 101.105, definition of Public Access Facility, Paragraph (1) says that the dock may <u>not</u> be primarily used for receiving vessels subject to part 104.

A dock that exists solely for the purpose of receiving a 104 vessel, cannot be considered a Public Access Facility. An example of this is as follows: A hotel has a dock that receives a 104 vessel. The dock has minimal infrastructure, but the public does not have access to the dock. The hotel restricts access to the dock to only those going aboard the vessel for a tour. Since the dock is only there because it is used to receive the 104 vessel, it falls under the requirement of 105, and cannot be considered a Public Access Facility.

5. If a Public Access Facility shares a boundary with a mall, hotel, stadium, or other such structure (that falls under the definition of facility in 101.105), the facility should coordinate security with that entity.

To minimize potential security gaps, for protection of the 104 vessel calling on the PAF, the facility should maintain an open dialogue with the adjoining structure. The PAF may need to know what security measures are in place at the stadium.

6. The boundaries of where to apply PAF security measures will be defined on a case by case basis in conjunction with the COTP/FMSC.

If a city riverfront dock is two miles long, and the 104 vessel only ties up to 100 feet of the riverfront, you may not necessarily need to apply the security to the entire two miles. The COTP/FMSC has the discretion to delineate the boundaries.

7. Some marinas could be considered a PAF.

If the marina dock receives a 104 vessel, and is not subject to 33 CFR 154, then it could meet the PAF definition. However, if the marina restricts access to their dock, then the dock does not have public access, and would not meet the definition of PAF but would be required to submit a facility security plan in accordance with 33 CFR Part 105 before receiving a vessel subject to part 104.

8. A restaurant with a dock that receives a 104 vessel could be a PAF.

9. City docks, city walk, river walk, inner harbor and other downtown waterfront areas typically meet the definition of PAF.

10. A facility, which only receives small passenger vessels (T boats), and does not receive 104 vessels, is not a 105 facility, and therefore is not considered a PAF.

These facilities will fall under the requirements of 101 and 103.

11. A facility that receives cruise ships, car ferries or passenger vessels regulated under SOLAS cannot be designated as PAF's, according to the PAF definition.

These facilities will fall under the requirements of 105.

12. If a location only receives a vessel one time, ever, this location would not be designated as a PAF. An example of this scenario would be a wedding at a backyard pier.

When a vessel goes to a dock only for a one-time event, such as a wedding, the facility should not be required to have a Facility Security Plan. At the same time, it is not feasible to designate the location as public access facility because the dock should not have to maintain these requirements all the time – the vessel is only going to be there once. Plus, if the dock is someone's private dock, and it only has a one-time visit, can the facility reasonably be expected to request a PAF designation? Will they even know about the requirements? The responsibility for security should fall on the vessel. For cases such as these, the vessel should request permission from the COTP/FMSC to tie up at a non-105 regulated facility by requesting a one-time waiver of the 105 facility regulations. The District Commander may grant a waiver of the 105 facility security regulations with input from the COTP/FMSC on a one-time basis only. Any subsequent requests for

waiver at the same facility must be forwarded to the Commandant (G-MP) for determination.

13. If a vessel makes a stop at a location with no infrastructure, this is not a PAF.

The example for this topic is a 104 vessel which stops at a riverbank and ties up to a tree stump. Another example would be a 104 vessel driving up on the beach. The definition of a facility is "any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction…." At a tree stump or on the beach, there is no structure. Since this is not a facility, it cannot be considered a PAF. The vessel should be held responsible for their security at this location. All of the elements of a DOS must be addressed by the vessel, since there is no "facility" there to cover any of the security measures. Even though a DOS is not required, the vessel shall still document the fact that they arrived at this location. This can be addressed in the Vessel Security Plan, or in the Area Maritime Security plan. The COTP/FMSC can spell out what security measures must be implemented at these locations, if needed.

14. A cruise ship arrives in a port and anchors away from the dock. The cruise ship uses their tender to ferry passengers back and forth to the dock, so that passengers may temporarily go ashore and return to the cruise ship. The dock has public access and has minimal infrastructure. Can the location be a Public Access Facility?

No, because the definition of a Public Access Facility says that these locations may not receive passenger vessels subject to SOLAS Chapter XI. The facility must be regulated under 33 CFR 105 and must submit a Facility Security Plan to receive SOLAS vessels. Or as an alternative, if they hire a local ferry or T-boat to shuttle passengers back and forth to the shore or PAF, the SOLAS tender will not arrive at the dock, and the 105 regulations will not apply. In this case, the vessel must ensure appropriate security measures are in place to ensure appropriate screening occurs when the passengers return. In regulating these 105 facilities, consideration should be given to waiving certain portions of the 105 requirements that relate to access control.

Company Letterhead

Date

U.S. Coast Guard
Marine Safety Office *(*Name*)*
Attn: Captain of the Port
Address
City, State, Zip

Dear Captain of the Port:

We request an exemption from the requirements of 33 CFR § 105. We believe our facility meets the definition of "public access facility" under 33 CFR § 101.105. [1] [*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*]

For your reference, we have conducted an abbreviated facility security assessment. [*Include results, which could consist of the following:*

Enclose diagram showing access points, both land and water

Enclose map of area showing highways, railroads, etc.

Security measures you and/or vessels will take during facility-vessel interface

Enclose photos of facility and surrounding area]

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*].

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*].

---

[1] § 101.105 Definitions.

Public access facility means a facility—

(1) That is used by the public primarily for purposes such as recreation, entertainment, retail, or tourism, and not for receiving vessels subject to part 104;

(2) That has minimal infrastructure for servicing vessels subject to part 104 of this chapter; and

(3) That receives only:

(i) Vessels not subject to part 104 of this chapter, or

(ii) Passenger vessels, except:

(A) Ferries certificated to carry vehicles;

(B) Cruise ships; or

(C) Passenger vessels subject to SOLAS Chapter XI

> I understand that under 33 CFR § 105.110, the Captain of the Port (COTP) may establish conditions for facility exemption from the requirements of 33 CFR § 105 to ensure adequate security is maintained. I further understand that under 33 CFR § 105.110, the COTP may withdraw the exemption for 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 exemption or any measure ordered by the COTP [pursuant to existing COTP authority].

Thank you for your consideration. If you have any further questions, you can reach me at [*your contact information*].

Sincerely,

*[*J. Smith*]*
Security Officer

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 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 designation PAF letter must inform the COTP and obtain approval prior to interfacing with a 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 104 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
Individual with Security Responsibilities		
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	

MARSEC I		
Maintain baseline security	X	

MARSEC II (When 104 regulated vessel at facility)		
Continue MARSEC I requirements	X	
Notify all facility personnel about identified threats and 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 104 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
Suspending access to the facility		X
Evacuating the facility		X
Restricting pedestrian or vehicular movement on the grounds of the facility		X
Increasing 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 cargo or 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

SENSITIVE SECURITY INFORMATION

U.S. Department of Homeland Security

United States Coast Guard

Captain of the Port
U. S. Coast Guard
Marine Safety Office

Xxxxxxx
Xxxxxxxx
xxxxxxxx
FAX: (xxx) xxx-xxxx

16600
Date

Facility Owner/Operator
Address
State

SUBJECT: PUBLIC ACCESS FACILITY DESIGNATION

(COMPANY NAME, FIN, MISLE ID #)

I have received your letter of dd/mm/yyyy requesting an exemption from the security regulation contained in 33 CFR 105. Taking into account the provisions of these regulations that allow for certain exemptions, and after evaluating your facility, I have determined that xxxx qualifies for an exemption. Your request for an exemption is therefore granted subject to continuing compliance with the conditions outlined below:

- Provide this office appropriate information for contacting the designated individual with security responsibilities for the Public Access Facility at all times;
- Comply with any Maritime Security (MARSEC) measures described in the Area Maritime Security Plan, all measures described in enclosure (1), and any Captain of the Port Orders requiring additional security measures, and
- Report any suspicious activities to the National Response Center at 1-800-424-8802.

As per 33 CFR Part 105.110(d)(3), the Captain of the Port may withdraw the exemption for a Public Access Facility at any time the owner or operator fails to comply with any requirement established as a condition of the exemption, or any measure ordered by the Captain of the Port.

You must be in full compliance with the above required measures by XXXXXX. This exemption will be evaluated annually to ensure the exemption remains 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.

I commend your continuing involvement with the Area Maritime Security Committee and the efforts you have undertaken to ensure the security of the port and the citizens of xxxxx. Please don't hesitate to contact xxx, of my staff, for any assistance.

Sincerely,

COTP Name
Rank, U.S. Coast Guard
Captain of the Port
Port Name

Encl: (1) Required Security Measures for Public Access Facility X [*List Specific Requirements*]

PUBLIC ACCESS FACILITY DESIGNATION
XXXX Facility

I acknowledge and accept the conditions of the exemption from the provisions of 33 CFR Part 105 documented in the Coast Guard Captain of the Port letter of xx/xx/xx. I will immediately inform the Captain of the Port of any changes of the operations at this facility that may affect this exempt status.

Signed: _____
Public Access Facility Owner/Operator

Signed: _____
Individual with Security Responsibilities

24 Hour contact information: _____

Date: _____

ENCLOSURE (3) TO NVIC 9-02 CHANGE 2

GUIDANCE FOR PORT SECURITY ASSESSMENTS

PORT SECURITY ASSESSMENT

BACKGROUND.

It is generally agreed that risk-based decision-making is one of the best tools to complete a security assessment and to determine appropriate security measures at a port. Risk-based decision-making is a systematic and analytical process to consider the likelihood that a security breach will endanger an asset, individual, or function and to identify actions to reduce the vulnerability and mitigate the consequences of a security breach.

Conceptually, risk can be represented as the product of the probability and consequence of a given security breach. This is represented by:

$R = P * C$

Where:

R = risk score for a given security breach
P = probability - probability of a security breach. The probability of a security breach can further be defined as the product of threat (T) and vulnerability (V).
C = consequence - the sum of possible consequences associated with a successful security breach. Consequences may be based on impacts to life, economic security, symbolic value, and national defense.

Risk management principles acknowledge that while risk generally cannot be eliminated, it can be reduced by adjusting operations to reduce consequence (C↓), threat (T↓), or vulnerability (V↓). Generally it is easier to reduce vulnerabilities than to reduce consequences or threats. The final goal of risk management is to achieve an adequately low and consistent level of risk. The goal for maritime security is to ensure that if the level of threat increases (T↑), either the consequences (C↓) or vulnerabilities (V↓) decrease to offset that increase. For example, a port may decide to increase security checks (V↓) after receiving a bomb threat (T↑). In another case, a vessel may be required to shift to a berth further away from buildings (C↓) during a shortage of security personnel (V↑).

DISCUSSION.

The key to risk-based decision-making is to correctly assess the value of risk. This requires four separate assessments: a criticality assessment, a threat assessment, a consequence assessment, and a vulnerability assessment.

A criticality assessment is a process designed to systematically identify and evaluate important assets and infrastructure in terms of various factors, such as the mission and significance of a target. For example, nuclear power plants, key bridges, and major computer networks might be identified as "critical" in terms of their importance to public safety, national security, and economic activity. In addition, facilities might be critical at certain times, but not others. For example, large sports stadiums, shopping malls, or office towers may represent an important target only when in use by large numbers of people. Criticality assessments are important

After criticality, threat, consequence, and vulnerability assessments have been completed and evaluated in this risk-based decision process, key actions can be taken to better prepare against potential terrorist attacks.

The following is a simplified risk-based security assessment that can be further refined and tailored to specific port facilities.

The overall steps of this security assessment are -

1. Perform a criticality assessment to identify critical activities or operations. This will lead to the identification of critical targets with the port. Table 1 provides an example for performing a criticality assessment of the targets. A blank worksheet is provided at the end of this enclosure.
2. Conduct a threat assessment to define scenarios by combining threats with credible attack scenarios. Table 2 lists some possible scenarios.
3. Conduct consequence and vulnerability assessments for each target/scenario combination using a high, medium, low score based on descriptors of specific elements in Tables 3 and 4. Table 3 lists several consequence elements to consider and Table 4 lists several vulnerability elements to consider. Note that consensus should be reached on a single overall consequence score and a single overall vulnerability score for each target/scenario combination.
4. Categorize the target/scenario combinations using Table 5. Table 5 prioritizes scenarios by organizing them into three categories: those for which mitigation strategies should be developed; those that should be considered on a case-by-case basis; and those that do not need mitigation strategies and need only to be documented.
5. Determine mitigation strategies and implementation methods using Tables 6 and 7. Strategies and methods need to consider the varying degrees of security threat (i.e., MARSEC levels).

An expanded explanation of the steps follows:

STEP 1: CRITICALITY ASSESSMENT

A Criticality Assessment will help identify activities and operations critical to a port. This will assist in target selection. Examples may include supporting a cruise line industry, ensuring throughput of needed precursors for a petrochemical industry, or providing waterway access for commuter ferries.

Identify those specific infrastructure targets that support critical operations of the port. All identified targets should be included in the evaluation. Targets considered, but dismissed for evaluation should be documented for future reference. While not all encompassing, the following table lists general classes of targets that should be considered. In addition, it is important to consider the role or mission of the target in the operation of the port. Broadly, we consider five mission or operation areas to be of interest. These are Public Health, Commerce, Safety/Defense, Transportation and Communications. The effect of destruction considers which consequence factors are affected by the loss of the target. The next consideration in determining

because they provide a basis for focusing the mitigation strategies and implementation methods on the most important items by identifying which assets and structures are more crucial to protect from an attack. Criticality assessments consider such factors as the importance of a structure to the missions of the port, the ability to reconstitute this capability, and the potential cost to repair or replace the asset. Criticality assessments should also give information on impacts to life, economic security, symbolic value and national defense. Criticality assessments provide information to prioritize assets and determine which potential targets merit further evaluation.

A threat assessment is used to evaluate the likelihood of attack against a given asset or location. It is a decision support tool that helps to establish and prioritize security-program requirements, planning, and resource allocations. A threat assessment identifies and evaluates each threat on the basis of various factors, including capability and intention. By identifying and assessing threats, organizations do not have to rely on worst-case scenarios to guide planning and resource allocations. Worst-case scenarios tend to focus on extreme consequences and typically require inordinate resources to address.

While threat assessments are a key decision support tool, it should be recognized that they are dependent on intelligence data. Even if updated often, threat assessments might not adequately capture emerging threats. No matter how much we know about potential threats, we will never know that we have identified every threat or that we have complete information even about the threats of which we are aware. Threat assessments alone are insufficient to support key judgments and decisions that must be made.

A consequence assessment evaluates the negative impact of a successful attack. It is a method to evaluate the likely outcomes of a scenario. The consequence analysis promotes the consideration of an attack's impacts including Deaths & Injuries, Economic, Public Safety/National Defense, Environmental, and Symbolic Effect. This assessment evaluates the consequence term of the risk equation.

A vulnerability assessment is a process that identifies weaknesses in physical structures, personnel protection systems, processes, or other areas that may lead to a security breach, and may suggest options to eliminate or mitigate those weaknesses. For example, a vulnerability assessment might reveal weaknesses in an organization's security systems or unprotected key infrastructure, such as water supplies, bridges, and tunnels. In general, teams of subject matter experts should conduct vulnerability assessments. For example, at many passenger terminals, experts have identified security concerns including the distance from parking lots to important staging areas and buildings as being so close that a car bomb detonation would damage or destroy the buildings and kill people in them. To mitigate this threat, experts have advised to increase the distance between parking lots and buildings. Another security enhancement might be to reinforce the windows in buildings to prevent glass from flying into the building if an explosion occurs. Such assessments can identify vulnerabilities in port operations, personnel security, and physical and technical security.

criticality is the ability to recover from destruction of the target. If an individual bridge is considered, but it is one of four parallel bridges crossing the same waterway, the ability of the port to recover from its destruction is likely to be better than if it is the only means. Finally, consider the number of mission areas affected, the degree of the effects and the ability to recover and make an overall assessment of the criticality.

Criticality should be rated according to the following scale: Critical/Moderate/Marginal. Critical items support multiple mission areas, have several consequence effects, and are difficult or impossible to recover from in a timely manner. Moderate criticality targets may support one or two missions areas, affect one or two consequence areas or have a reasonable ability to recover in a timely manner. Marginal criticality targets may not support any mission areas, may have limited to minimal effects of destruction and may have back-up or redundant systems in place that minimize recovery time.

Table 1: Criticality Assessment

Target	Mission	Effect of Target Destruction	Ability to Recover	Criticality
Bridge Utility Pier Tunnel Waterway Other	*Public Health Commerce Safety / Defense Transportation Communications Other*	*Loss of Life Economic Impact Environmental Impact Public Safety / Defense Symbolic Significance*	*Excellent Good Fair Poor None*	*Critical Moderate Marginal*

When feasible it is preferable to group identical targets at the specific target level. However, some targets may need to be considered individually. For example, a unique bridge should be considered individually given differences in communication cables, pipelines, and traffic. The purpose of considering targets individually is to be specific enough to differentiate which targets need mitigation.

Large facilities such as Port Authorities may be considered as one target or subdivided into individual targets as appropriate based on the attack scenario. For example, an entire Port Authority may be the target in one attack scenario, but individual parts of it may be targets in other attack scenarios.

STEP 2: THREAT ASSESSMENT AND SCENARIO SELECTION

An attack scenario consists of a potential threat to a unique target or target class under specific circumstances. It is important that the developed scenario or scenarios are within the realm of possibility and, at a minimum, address known capabilities and intents as evidenced by past events and available intelligence. For example, a boat containing explosives (a specific class of scenario) ramming a tanker (target) that is outbound through a choke point (specific circumstance) is one credible scenario. It is much less credible that a U. S. Navy ship will be

commandeered and used to ram a bridge unless specific intelligence reports indicate otherwise. Table 2 provides a notional list of scenarios that may be combined with specific critical targets to develop the scenarios to be evaluated in the Port Security Assessment.

Table 2: Notional List of Scenarios

Typical Types of Scenarios		Application Example
1. Intrude and/or take control of the target and ...	1.a Damage/destroy the target with explosives	Intruder plants explosives.
	1.b Damage/destroy the target through malicious operations/acts	Intruder takes control of a vessel and runs it aground or collides with something intentionally. Intruder intentionally opens valves to release hazmat, etc.
	1.c Create a hazardous or pollution incident without destroying the target	Intruder opens valves/vents to release toxic materials or releases toxic material brought along. Intruder overrides interlocks leading to damage/destruction.
	1.d Take hostages/kill people	Goal of the intruder is to kill people.
2. Externally attack the target by …	2.a Moving explosives adjacent to target - From the waterside - On the shore side - Subsurface	USS Cole style attack. Car/truck bomb.
	2.b Ramming a stationary target: - With a vessel - With a land-based vehicle	Intentional allision meant to damage/destroy the target (i.e., waterway choke point). NOTE: Evaluate overall consequences from the allision, but only evaluate the vulnerabilities of the target and not the vulnerabilities of the vessel/vehicle used to ram the target.
	2.c Launching or shooting weapons from a distance	Shooting at a target using a rifle, missile, etc.
3. Use the target as a means of transferring …	3.a Materials, contraband, and/or cash into/out of the country	
	3.b People into/out of the country	

A target may prompt a few or many scenarios. The number of scenarios is left to the judgment of the AMS Committee. A thorough initial evaluation should be possible with less than 100 target-scenario combinations. Care should be taken to avoid unnecessarily evaluating excessive numbers of similar scenarios or those that result in low consequences. That is why a criticality assessment should be performed initially to focus efforts on critical targets. Minor variations of the same scenario also do not need to be evaluated separately unless there are measurable

differences in consequences or vulnerabilities. A worksheet at the end of this enclosure provides a suggested method for capturing the Port Security Assessment information.

STEP 3: CONDUCTING A CONSEQUENCE AND VULNERABILITY ASSESSMENT

In this step each target/attack scenario combination will be evaluated in terms of the potential consequences of the attack and the vulnerability (or invulnerability) of the target to the attack.

Five elements are included in the consequence assessment: death and injury, economic impact, environmental impact, national defense impact, and symbolic effect. A descriptor of the consequence components follows in Table 3.

Table 3: Consequence Categories

DEATH AND INJURY	The prospective number of lives lost and injuries occurring as a result of an attack scenario.
ECONOMIC IMPACT	The potential economic impact of an attack scenario.
ENVIRONMENTAL IMPACT	The potential environmental impact of an attack scenario.
PUBLIC SAFETY/ DEFENSE IMPACT	The potential effect on public safety/ defense resulting from an attack scenario on different targets, including Department of Defense (DOD) targets.
SYMBOLIC EFFECT	The potential that the target is closely linked as a symbol with the American economy, political system, military, or public welfare.

Individual consequence elements for a given scenario need to be addressed but should be summarized into a single score for each target/scenario combination: high, medium or low.

Consequence categories and criteria with benchmark examples are provided in Table 4. The committee can alter the scoring criteria in Table 4 to accurately reflect the physical characteristics and activity in the area being assessed (e.g. > 100 deaths or serious injury vice >1000 for a rating of high), but any changes and their rationale should be clearly documented.

Table 4: Consequence Score

	Death/ Injury	Economic Impact	Environmental Impact	National Defense	Symbolic Effect
High	>1,000 deaths or serious injuries	>$US 100 million	Complete destruction of multiple aspects of the eco-system over a large area	Creates critical long-term vulnerabilities in public safety/ defense	Major damage of nationally important symbols that are internationally recognized
Medium	1,000 to 100 deaths or serious injuries	From $US 10 to 100 million	Long-term damage to a portion of the eco-system	Short-term disruptions in public safety/ defense	Major damage or destruction of regionally or locally important symbols
Low	0 to 100 deaths or serious injuries	< $US 10 million	Small spills with minimal, localized impact on the eco-system	No serious safety/defense impact	Minor/no damage to an important symbol

Four elements of vulnerability are included in the computation of the vulnerability score: availability, accessibility, organic security, and target hardness. A descriptor of the vulnerability components follows in Table 5.

Table 5: Vulnerability Categories

AVAILABILITY	The target's presence and predictability as it relates to the ability to plan an attack.
ACCESSIBILITY	Accessibility of the target to the attack scenario. This relates to physical and geographic barriers that deter the threat without organic security.
ORGANIC SECURITY	The ability of security personnel to deter the attack. It includes security plans, communication capabilities, guard force, intrusion detection systems, and timeliness of outside law enforcement to prevent the attack.
TARGET HARDNESS	The ability of the target to withstand the specific attack based on the complexity of target design and material construction characteristics.

The committee should discuss each vulnerability element for a given scenario but should summarize the discussion into a single score for each target/scenario combination; high, medium or low. The initial evaluation of vulnerability should be viewed *without* new strategies meant to lessen vulnerabilities, even if there are strategies already in place. For future reference, the organic security components already being used should be noted. Assessing the vulnerability without strategies will provide a more accurate baseline score of the overall risk associated with the scenario. After the initial evaluation has been performed, a comparison evaluation can be made *with* new strategies considered. Vulnerability categories and criteria are provided in Table 6.

Table 6 Vulnerability Score

Category	Availability	Accessibility	Organic Security	Target Hardness
High	Always available (e.g., continually present or present daily on a set schedule)	No deterrence (e.g., unrestricted access to target and unrestricted internal movement)	No deterrence capability (e.g., no plan, no guard force, no emergency communication, outside L. E. [law enforcement]) not available for timely prevention, no detection capability	Intent of attack easily accomplished (e.g., readily damaged or destroyed)
Medium	Often available (e.g., present several times a month; arrival times predictable 1 week to 2 months in advance; predictable departure times)	Good deterrence (e.g., single substantial barrier; unrestricted access to within 100 yd of target)	Good deterrence capability (e.g., minimal security plan, some communications, armed guard force of limited size relative to the target; outside L. E. not available for timely prevention, limited detection systems)	Good ability to withstand attack (e.g., simple design but relatively strong construction)
Low	Rarely available (e.g., no set schedule and on any given day presence highly unlikely and unpredictable; arrives once a year or less for a few hours and arrival is not publicly known)	Excellent deterrence (expected to deter attack; access restricted to within 500 yd of target; multiple physical/geographical barriers)	Excellent deterrence capability expected to deter attack; covert security elements that represent additional elements not visible or apparent)	Target expected to withstand attack (e.g., complex design and substantial construction of target minimizes success of attack)

STEP 4: CATEGORIZING THE TARGET/SCENARIO COMBINATIONS

The team should next determine which scenarios should have mitigation strategies identified by determining where the target/scenario combination falls in Table 7 based on the consequence and vulnerability assessment scores.

Table 7. Vulnerability & Consequence Matrix

		Vulnerability Score		
		Low	**Medium**	**High**
Consequence Score	**High**	**Consider**	**Mitigate**	**Mitigate**
	Medium	**Document**	**Consider**	**Mitigate**
	Low	**Document**	**Document**	**Document**

"Mitigate" means that mitigation strategies should be developed to reduce risk for that target/scenario combination. A security plan should contain the scenario evaluated, the results of the evaluation and the mitigation measures.

"Consider" means that the target/scenario combination should be considered and mitigation strategies should be developed on a case-by-case basis. The port security plan should contain the scenario evaluated, the results of the evaluation, and the reason mitigation measures were or were not chosen.

"Document" means that the target/scenario combination does not need a mitigation measure at this time and therefore need only to be documented. The security plan should contain the scenario evaluated and the results of the evaluation. This will be beneficial in further revisions of the security plan, in order to know if the underlying assumptions have changed since the last edition of the security assessment.

STEP 5: DETERMINING MITIGATION STRATEGIES AND IMPLEMENTATION METHODS

The true value of these assessments is realized when mitigation strategies are implemented to reduce consequences and vulnerabilities. The desire is to reduce the overall risk associated with the identified target/scenario combinations. Note that, generally, it is often easier to reduce vulnerabilities than to reduce consequences or threats when considering mitigation strategies.

As an example of a possible vulnerability mitigation measure, a company may contract for a stand-by tug to provide "sentry duty" to prevent ramming of a cruise ship. This measure would improve organic security and may reduce the overall vulnerability score from a "high" to a "medium." However this option is specific for this scenario and also carries a certain cost. Another option might be to dock the cruise ship in a more protected berth. This may reduce the accessibility score from "high" to "medium". This option may not require additional assets, but reduces the risk of this scenario, and may even provide mitigation for additional scenarios. Similarly, other scenarios can be tested to determine the most effective strategies.

The AMS Committee should develop a process through which it continually evaluates the overall security by considering consequences and vulnerabilities, how they may change over time, and what additional mitigation strategies can be applied. The committee should organize strategies according to general categories. For example, Table 8 provides a notional list of general categories along with the goal those strategies should meet.

Table 8: General Strategies and Goals for Risk Reduction

Category	Goal
Maritime Domain Awareness (MDA)	Knowledge from origin to final destination of all activities, forces, and elements that influence safety, security, economy, or environment of the port. MDA is based on a foundation of information collection, analysis, fusion, and sharing.
Command, Control, Communication, & Coordination (C4)	Effective vessel/port/facility stakeholder, appropriate government agencies, emergency service providers. C4 maintains awareness, sustained operations, and the security and safety of the port.
Access Control	Processes and physical means that ensure security for access to and within the port and vessels.
Plans, Policies, and Procedures	Risk assessments and processes that reduce risk by deterring security breaches and eliminate or minimize consequences or threats.
Critical Infrastructure	Protection of critical infrastructure to include national security interests.
Cargo Control	Processes and physical means that ensure the security of imported/exported cargo.
Passenger / Crew and MISC Vessel Control	Processes and physical means that ensure passenger/employee safety and security.
Crisis / Consequence Management	Response to security breach and management of the consequences (e.g., injury, death, port damage, or destruction, etc.).

Tables 9 and 10 are intended to assist the AMS Committee in developing and selecting mitigation strategies and are categorized by the previously mentioned categories. They offer examples in developing mitigation strategies. Note that there may be more than one strategy under each category.

The AMS Committee should brainstorm strategies and record all strategies in a table such as Table 9. Strategies must then be ranked in terms of effectiveness and feasibility. Using a table similar to Table 10 will assist the committee in ranking strategies.

A strategy may be thought of as effective if its implementation lowers the overall consequence or vulnerability score. A strategy may be thought of as partially effective if the strategy will lower an overall score when implemented along with one or more other strategies. A strategy may be thought of as having no effect if its implementation does not lower a score.

A strategy may be thought of as feasible if it can be implemented with little trouble or funding within current budgetary constraints. A strategy may be thought of as partially feasible if its implementation requires significant changes or additional funding. A strategy may be thought of as not feasible if its implementation is problematic or is cost prohibitive except under extreme threat conditions.

The committee should keep in mind that strategies must be deployed commensurate with various security threat levels established and set by the appropriate government agency. Effective strategies that are feasible should be considered for implementation at the lowest security threat level. Effective but partially feasible strategies may be implemented during higher security threat levels. Strategies must ultimately maintain, to the utmost, an equivalent level of security despite changes in security threat levels.

After the selection of the mitigation strategies and implementation methods, the PSC should check the results to ensure that critical operations are maintained and the risk is reduced to the port. Some mitigation strategies might include shutting down non-critical operations during higher threats.

Table 9: Mitigation Strategy Development Worksheet – EXAMPLE

Target:	**Mitigation Strategy**							Strategy Reduces:	
Scenario	**Maritime Domain Awareness**	**Command, Control, Communication, & Coordination (C4)**	**Access Control**	**Plans, Policies, and Procedures**	**Critical Infrastructure**	**Cargo Control**	**Passenger/Crew and MISC Vessel Control**	**Vulnerability**	**Consequence**
Intentional sinking of cruise vessel while embarking/ disembarking passengers	Requires vessel to post lookouts while moored.							X	
		Receives and communicates emergent threat information						X	X
			Requires small boat patrol on waterside					X	
				Has identified adequate medical & law enforcement response personnel in case of attack					X
							Restricts non-essential personnel from area close to passenger terminal	X	

Table 10: Mitigation Strategy Benefit Analysis – EXAMPLE

Target: Cruise Liner	**Scenario:** Intentional Sinking											
	Effective			Feasible			Apply in threat level :				Resources	
Strategy	**Yes**	**Partially**	**No**	**Yes**	**Partially**	**No**	**Low**	**Med**	**High**	**None**	**Available**	**Gap**
Armed lookouts		x			x			x	x			
Emergent threat information		x			x			x	x			
Small boat patrol	x					x			x			
Adequate response personnel	x				x		x	x	x			
Restrict non-essential personnel	x			x			x	x	x			

Port Security Assessment

Target	Scenario	Criticality	Consequence	Vulnerability	Action
		Critical Moderate Marginal	*High Medium Low*	*High Medium Low*	*Mitigate Consider Document*

ENCLOSURE (4) TO NVIC 9-02 CHANGE 2

GUIDANCE FOR THE AREA MARITIME SECURITY PLAN EXERCISE PROGRAM

ENCLOSURE (4) TO NVIC 9-02 CHANGE 2

GUIDANCE FOR THE AREA MARITIME SECURITY PLAN EXERCISE PROGRAM

TABLE OF CONTENTS

1. **PURPOSE**.

This enclosure provides guidance to Coast Guard Captains of the Port (COTP)/Federal Maritime Security Coordinators (FMSC) and Area Maritime Security Committees (AMSC) in carrying out their collective responsibility to conduct or participate in annual exercises to test Area Maritime Security Plans (AMSP).

2. **BACKGROUND**.

In accordance with the Maritime Transportation Security Act of 2002 (MTSA) regulations in 33 CFR 105.515, COTPs and AMSCs shall ensure that exercises to test the effectiveness of the AMS Plan are carried out once each calendar year, with no more than eighteen months between exercises. As a critical element in the Plan-Train-Exercise-Evaluate-Document preparedness cycle, these exercises are a mechanism by which FMSCs and AMSCs can continuously improve preparedness by validating information and procedures in the AMS Plan, identify weaknesses (for correction in subsequent versions of the AMS Plan), identify strengths (to share as best practices), and practice command and control within an incident command/unified command framework.

Initial versions of the Area Maritime Security Plans were completed in the spring of 2004. Thus, for the first round of exercise requirements, AMSCs must conduct or participate in an AMS exercise prior to December 31, 2005. Subsequent exercises must meet the provisions of 33 CFR 103.515.

Two types of exercises will be conducted to meet the MTSA requirements. Triennial Full Scale Exercises (FSX), referred to as field training exercises in 33 CFR 103, are large, comprehensive exercises that will typically involve multiple agencies and may assess security incidents as well as other types of contingencies. Each AMSP must be exercised in this manner once every three years. When possible, these exercises may be included as part of a larger national exercise (such as TOPOFF).

Annual exercises are smaller, focused exercises that will be conducted each year (with no longer than eighteen months between exercises) for each AMSP. While the regulation allows for the annual exercise to be conducted as an FSX or Table Top Exercise (TTX), it is envisioned that the exercises conducted in the non-triennial FSX years will be TTXs or Command Post Exercises (CPX). They are primarily used by port level organizations for training, assessing preparedness, and testing the adequacy of the AMSP for specific functions (e.g. Communications, C2, Logistics, etc.).

3. **DISCUSSION**

Area Maritime Security Committees, in coordination with the Federal Maritime Security Coordinators, must be prepared to prevent, protect and respond to all potential security threats to their local port communities. The AMSC must conduct preparedness, response and training operations in support of national security policy objectives. These objectives will be supported through awareness, prevention, detection, protection, response and recovery activities at all

levels of threat intensity within the spectrum of maritime transportation security. Logistical support must also be identified. Members of the AMSC must be ready to manage all manner of threats and security incidents in all port areas, as well as react as necessary to incidents in areas adjacent to the port that may impact the port (i.e. the buffer zone).

The AMS exercise program is intended to challenge port resources and terrorism prevention measures through the development of, and response to, realistic scenarios to determine if the AMS Plan accurately addresses the needs of the port. To achieve this goal, a continuous process is set in motion, beginning with the port risk assessment, continuing with planning and exercises, and culminating in the development of valuable lessons learned and best practices. Lessons learned are used to improve AMS Plans, and best practices are shared with other ports to improve security posture. The purpose of AMS exercises is to improve the AMS Plan and create a product that ensures the security of the marine transportation system.

There are currently two guiding documents for use by AMSCs/FMSCs in developing and executing AMS exercises. Existing Coast Guard exercise management guidance exists in COMDTINST M3010.13B, Contingency Planning Preparedness Manual Volume III - Exercise Policy and Planning (CPPM Vol. III). The Department of Homeland Security's doctrine is contained in the Homeland Security Exercise and Evaluation Program (HSEEP), which is becoming widely used by state and local officials as well as other DHS agencies for homeland security exercise program management.

The HSEEP is both doctrine and policy for designing, developing, conducting and evaluating exercises. HSEEP is a threat- and performance-based exercise program that includes a cycle, mix and range of exercise activities of varying degrees of complexity and interaction. HSEEP includes a series of four reference manuals to help states and local jurisdictions establish exercise programs and design, develop, conduct, and evaluate exercises. Volume I: Overview and Doctrine (Revised), provides requirements and guidance for the establishment and maintenance of an exercise and evaluation program. Volume II: Exercise Evaluation and Improvement, offers proven methodology for evaluating homeland security exercises and implementing an improvement program. Volume III: Exercise Program Management and Exercise Planning Process, helps planners establish an exercise program and outlines a standardized design, development, conduct, and evaluation process adaptable to any type of exercise. Volume IV: Sample Exercise Documents and Formats, provides sample exercise materials referenced in HSEEP Volumes I–III. HSEEP documents are available on the Office of Domestic Preparedness (ODP) website at http://www.ojp.usdoj.gov/odp/docs/hseep.htm.

CPPM Vol. III is a combined two-part document that describes the Coast Guard's policy and doctrine for planning and conducting contingency exercises. Chapters 1 through 3 contain policy and doctrine, and Chapters 4 through 9 encompass the procedures to be used in planning and conducting an exercise. It is an excellent guide for an exercise planner or participant and discusses in detail the planning philosophy from beginning to end. CPPM Vol. III is available on

the CG Intranet at http://cgweb.comdt.uscg.mil/G-OPF/opf3/Web%20Pages/cpdocs.htm. Both the CPPM and HSEEP shall be shared amongst the AMSC through the local Coast Guard Planning Officer. The CPPM and HSEEP are consistent in terms of underlying principles; both provide general but comprehensive guidelines and processes for development and execution of exercises. Both documents shall be referenced for development of an AMS exercise program, and throughout the exercise design process.

This enclosure will not repeat existing exercise development/execution doctrine but will rather provide expectations and additional guidance specific to planning and conducting AMS Plan exercises. It also discusses training concepts to be contemplated and incorporated by AMSCs/FMSCs in the AMS preparedness cycle. The enclosure is written for AMSCs, FMSCs and their staffs, as well as exercise planners, primarily at sector/port level and below.

4. THE AMS EXERCISE PROGRAM.

4.1. Goals of the Area Maritime Security Exercise Program

AMS exercises are an integral part of a coordinated, comprehensive homeland security exercise program, and will align with, and support, the National Preparedness Goal, the National Maritime Security Plan (NMSP), and the National Exercise Program.

The Department's National Preparedness Goal, the National Preparedness System Description, and National Planning Guidance are under development and/or evolving within DHS. As these documents are finalized, they will continue to set expectations and standards by which homeland security preparedness will be measured. Accordingly, they will continue to inform future policy and efforts regarding AMS Plan and AMS exercise program content.

The following are overarching strategic goals for the AMS Exercise Program:

- Assess the adequacy of the AMS Plan to prevent acts of terrorism.
- Assess the adequacy of the AMS Plan to implement and conduct coordinated interagency command and control operations in accordance with the National Incident Management System (NIMS).
- Assess the adequacy of the AMS Plan to effectively communicate between various federal, state, and local agencies as well as industry stakeholders, across all affected modes of transportation (while engaged in the prevention of, response to, or recovery from a transportation security incident (TSI)).
- Assess the adequacy of the AMS Plan to facilitate sharing, correlating, and disseminating information and intelligence (including sensitive security information (SSI)) amongst the members of the AMSC to prevent or effectively respond to an act of terrorism.
- Validate port security risk assessments and identification of critical infrastructure within the port.
- Assess the adequacy of the AMS Plan to facilitate attainment of MARSEC levels as directed.

- Assess the adequacy of the AMS Plan to prepare appropriate stakeholders in the FMSC's AOR to respond to, and mitigate a TSI, including linkages to appropriate incident management/response plans.
- Assess the adequacy of the AMS Plan to facilitate recovery from an act of terrorism and restore key transportation services and critical infrastructure within the affected port.

4.2. **Roles and Responsibilities**

The AMSC will be heavily involved in ensuring all phases of the AMS preparedness cycle are addressed. It is strongly recommended that AMSCs establish Exercise Subcommittees to focus on scheduling, planning, conducting, and evaluating exercises to support the AMS Plan and to help guide overall port security preparedness efforts. Members of the AMS Exercise Subcommittee will become well versed in homeland security preparedness doctrine as well as exercise program management principles. These individuals then become natural selections to participate in various stages of exercise development such as exercise design teams, evaluation teams, etc.

Roles as they relate to AMS Exercises are as follows:

Triennial Full Scale Exercises (FSX):
Exercise Sponsor – Commandant
Exercise Director – Area Commander
Design Team/Evaluation Coordinator – Area Commander and District Commander
Design/Control/Evaluation Teams – Area Commander and District Commander
Subject Matter Experts for Exercise Design – FMSC, AMSC Members and port stakeholders

Annual Exercises (TTX/CPX):
Exercise Sponsor – Commandant and Area Commander
Exercise Director – District Commander and FMSC/AMSC Members
Design Team/Evaluation Coordinator – District Commander and FMSC/AMSC Members
Design/Control/Evaluation Teams - District Commander and FMSC/AMSC Members
Subject Matter Experts for Exercise Design – FMSC, AMSC Members and port stakeholders

4.3. **Exercise Content Requirements**

Section 5.4 below contains specific Major and Supporting Objectives for AMS Exercises which are based on AMS Plan contents and the strategic objectives outlined above. There are four Major Objectives for AMS Exercises; they cover the areas of Awareness, Prevention, Response and Recovery. Since it may not be practicable to assess all objectives (i.e. all areas of the AMS Plan) comprehensively during any particular exercise, the following provides guidance on sufficiency of AMS exercises to meet the intent of the program.

Annual Exercises: These exercises must include core components from at least two of the four Major Objectives. AMSCs/FMSCs shall choose objectives to be tested based on the needs of the port community in terms of its preparedness and the state of the AMS Plan (see Section 5.1

below regarding Needs Assessments). The core components of all four AMS exercise program Major Objectives must be exercised over a 3-year period**.**

Triennial Full Scale Exercises: These exercises must include core components from at least three of the four Major Objective areas. Additionally, they must include (1) Activation of an incident command/unified command structure; and (2) field deployment of security resources in response to significant increases in threat information, MARSEC level changes, and/or a transportation security incident.

The general nature of the exercise requirements is intended to provide maximum flexibility to AMSCs/FMSCs in planning and designing exercises to best suit the needs of the port, as well as to facilitate combining exercises with other agencies or entities.

4.4. **Scheduling AMS Exercises**

A growing number of agencies and entities, at all levels of government and the private sector, are becoming involved in the development and execution of homeland security exercises and exercise programs. Many of these exercises require the participation of the same agencies and entities. In order to achieve economies of scale, and best utilize scarce resources, personnel at all levels should look for opportunities, where feasible, to pool resources to combine and conduct homeland security exercises that meet the goals and objectives of the various programs.

The regulations require the COTP to coordinate with the AMSC to conduct or participate in an Area Maritime Security Exercise at least once each calendar year, with no more than 18 months between exercises.

AMS Exercises must continue to be scheduled in the CG's Contingency Preparedness System (CPS) per the CPPM, allowing CG Program Managers to maintain the national exercise picture and assist in coordination with other federal agencies. CG Program Managers project CG exercises out for 5 years for coordination amongst external exercise programs, therefore the FMSC will be responsible for scheduling all AMS exercises, projecting out also, on a five-year schedule. Each unit shall schedule all required AMS exercises for the coming 5 fiscal years and enter with a concept of exercise (COE) in CPS by the end of June every calendar year.

The purpose of the five-year schedule is to enable exercise program managers at all levels to plan for and coordinate upcoming exercise activities, including funding allocations. As such, the schedule is not intended to be one hundred percent accurate for all three years. In a five year cycle, the first year should be 90 percent accurate, the second year 85 percent accurate, and the third year 75 percent accurate. Years four and five should be thought of as place holders. The COEs should reflect this accuracy projection. The first year COE shall be robust and detailed and include all aspects of exercise play, with the follow-on year's COE being less specific. Area Commanders will review the Units' submissions and work with Contingency Planning and Exercise Program Managers to reconcile and finalize the five year schedule by September of each year, engaging Departmental partners in the process.

The CPS entries will be used to fill a national five-year schedule promulgated by HQ Program Managers (will include FSXs only) for inclusion into the National Exercise Schedule (NEX), and will allow Area and District Commanders to negotiate CG participation in exercise programs sponsored by non-USCG entities. The NEX is maintained by DHS and can be found on their secure, web-based portal. For "view" access to the National Exercise Schedule, members may call the Centralized Scheduling and Information Desk (SCID) Help Line at 1-800-368-6498.

4.5. **Identification of Resources**

4.5.1. Exercise Funding

Funding for AMSP exercises will be provided to Areas by G-MP on an annual basis based on a standard budget model. Release of AMSP Exercise funds is contingent on LANT and PAC Area (m) and (p) staffs verifying that COEs have been prepared and submitted for all required AMSP exercises which a unit is to conduct as outlined in their five-year schedule. The COEs for the first year should include full details regarding exercise play. The COEs for the follow on years are expected to be much less detailed, but should include intended private sector involvement and major exercise objectives. Funds are intended to support the overall preparedness cycle as well as the specific exercise. Frequently asked questions regarding expenditure of CG provided exercise funds are included as Tab A to this document.

The TSA sponsored Port Security Training and Exercise Program (PortSTEP) will be conducted under the auspices of the AMSP exercise program [1]. Funding for CG participation in these exercises will normally be provided to Areas by G-MP. Units involved in PortSTEP exercises are reminded that all relevant PortSTEP exercise activities must be recorded in CPS as noted elsewhere in this document.

Whenever possible AMSCs should investigate and consider all sources of funding and resources to support the AMS Exercise Program including opportunities to combine HSEEP and AMS exercise funds. AMSCs may also wish to routinely review the National Exercise Schedule to take advantage of opportunities to participate in other exercises and to avoid conflicts with events conducted under the HSEEP exercise program. State and Local governments (members of the AMSCs) have avenues to receive exercise funding, including funds distributed through the DHS port security grant program. Chapter 1 of the HSEEP provides more detailed guidance on these avenues. It must be noted that funding through HSEEP requires that exercises be conducted in accordance with HSEEP doctrine.

4.5.2. Exercise Support

In addition to funding support, G-MP is working to identify staff support for exercise development, conduct, and evaluation. All options will be considered. In addition to contractor

[1] PortSTEP is currently a finite program ending in FY 2007, and will exercise 40 port communities. Specific guidance on this program is outlined for AMSCs and port communities in other documents.

support for exercise development and execution, development of a cadre of preparedness and exercise subject matter experts from all levels of the organization, including CGHQ, the NSFCC, Areas, Districts, local units, as well as other agencies within DHS to support various exercise activities is being considered.

In terms of planning and execution of AMS exercises, the Coast Guard's long term vision is to identify qualified, proficient contractor support to facilitate FSXs at the AMSC level. Contractor support for FSXs will be developed and available during FY 2006. G-MP will initiate and maintain a Statement of Work (SOW) for the contractors. The Area Commanders, working with the District Commander and FMSC, will work with the contractors to schedule FSX support, and complete individual task orders (TO) for each exercise. The TO will specify the needs of the AMSC for a particular FSX. Detailed guidance will follow when this process is finalized, projected early in FY 2006.

Contractor support for AMS exercises is also being provided to specified FMSCs through the TSA funded PortSTEP program (again, a finite program spanning from 2005-2007).

The intent is also to develop a pool of qualified subject matter experts and evaluators at the national level available for support or consultation. The AMSC or District would request services in the course of exercise planning. The HQ program managers and Areas will coordinate this national pool of evaluators and "assign" personnel as requests flow up from AMSCs and Districts.

Support for training is addressed in Section 5.2 of this document.

4.6. **Supplemental Guidance**

Basic exercise development processes are outlined in CPPM Vol. III and HSEEP, and the steps are outlined below. The following sections provide guidance to supplement various stages of the process, specific to AMS Exercises. The sections are organized into Pre-Exercise and Post-Exercise activities. Also, information on obtaining AMS exercise credit for other exercises and real world events, as well as public affairs, is included.

Basic Exercise Development Process

1. Review the plan(s)
2. Conduct a Needs Assessment
3. Determine the scope of the exercise
4. Draft Concept of Exercise
5. Develop the planning timeline
6. Transmit the Exercise Directive to the appropriate personnel
7. Refine Concept of Exercise and enter into CPS; continue to refine as planning process evolves
8. Organize the Exercise Evaluation Subcommittee
9. Prepare Exercise Major and Supporting Objectives

10. Prepare the Master Scenario Events Listing (MSEL), along with the Exercise Narrative
11. Include major and detailed events, along with expected actions
12. Finalize Exercise Enhancements
13. Develop the Exercise Evaluation Data and Collection Plan (ED&CP) format
14. Conduct the Exercise
15. Conduct the Post-Exercise Meeting (Hot Wash)
16. Prepare After-Action Report and lessons learned and enter into CPS.
17. Conduct any other follow-up activities

5. **PRE-EXERCISE ACTIVITIES**

5.1. **Needs Assessment**

Before the exercise development can begin, the AMSC must determine its needs and capabilities. This determination may be met by a formal or informal capabilities or readiness assessment. A solid training program will identify the level of qualification and knowledge of the participants. Other factors that shall be considered before commencing the exercise planning include available funds, available space, geographical or climatological influences, scheduling conflicts/ participant availability, last review date of the plan, mandated exercise requirements, rotation or influx of new personnel/ stakeholders, etc.

One or more of these factors can dictate what type of exercise will be conducted. Therefore it is important that a solid assessment of both the current level of preparedness of the port community and the current logistical capabilities are known. For example if money and facilities are limited, and the AMSP has not been recently reviewed, it may be a good decision to conduct a TTX. This type of exercise may also be beneficial when participants have limited knowledge and training due to recent assignment or transfers. An FSX may be considered when the AMSP has recently been validated and the AMSC feels comfortable with the competency of exercise participants. The value of exercise planning relies both on knowledge of the current training level and a comprehensive review of the influencing factors above.

5.2. **Training**

Training is a key component in the preparedness cycle, and an ongoing part of the planning process. Training should be conducted on an ongoing basis to enhance and sustain readiness for actual incidents. The AMSC and FMSC will identify training necessary to enhance specific community, as well as individual, knowledge and skills. The diversity of organizations, equipment, and environment inherent in the maritime security community presents a major challenge to incident response managers. They must train community members and leaders who can effectively integrate the community's preparedness systems and doctrine to defeat an enemy that may be totally asymmetric or unconventional in nature. Training by conducting security preparedness exercises, is an effective way to build the teamwork necessary to meet this challenge.

Training considerations for AMS Exercises include:

Command and Control Skills:
Command and control training sustains skill proficiency for incident managers, leaders, staffs, and individual community members. It reinforces common incident command system (ICS) skills and those particular to duty positions. It trains each echelon to respond to the needs of higher, lower, adjacent, and temporarily present elements. Doctrine and training support materials for command and control training include such items as scenarios, simulation models, and recommended task lists. The AMSC can adapt these materials to address its unique capabilities assessment.

To best manage security preparedness, all elements of the AMSC must be integrated and need to function effectively during periods of heightened threats. Critical decision makers must be competent in their command and control tasks. Unified commands must be proficient in executing staff planning responsibilities to achieve full integration of supporting elements and services. Training that enhances these skills will receive emphasis at AMSC level and above. The three categories of command and control training are unified command training, survivability training, and systems integration training.

Unified Command Training- develops the proficiency of individual staff members and molds them into trained teams that can effectively manage and coordinate all systems to support the incident management process.

Survivability Training- ensures proficiency during intense and continuous heightened periods of threat. It ensures that individuals and teams can operate effectively in a variety of situations. It involves those routine tasks that communities must perform well to ensure their survival. Examples include:

- Operations in nuclear, biological, or chemical (NBC) environments.
- Operations in hostile takeovers or indiscriminant targeting (snipers).
- Operations using various command post (CP) configurations.
- Procedures for succession of command.
- Limited visibility operations.
- Activation of alternate communication methods.
- Activation of alternate command posts.
- The hand-off between command posts (tactical CP to main CP).
- Local security.

Systems Integration- ensures stakeholders and responders work cohesively, and communications links are optimized. Examples include:

- Intelligence and information sharing.
- Information technology and information/knowledge management.
- Waterways management.

Operational (Tactical) Doctrine and Skills for Field Forces - consider different agencies who may provide field forces, differing tactical or operational policies, identification of common practices and procedures for joint operations. Examples include:

- Enforcement of waterside security zones
- Enforcement of restricted areas landside
- Multi-Agency Vessel Boardings
- Use of Force

The doctrine provided in the Department's National Preparedness Goal, National Preparedness System Description, and the National Planning Guidance is expected to further refine appropriate types of training necessary to build skills to meet national preparedness requirements.

The FMSC or AMSC may identify a need to enhance special skills or teamwork aspects as a precursor to actual exercise events. With the exception of web-based training, requests for the services below shall follow the normal chain of command. Training funding requests related to the conduct of an AMS exercise shall be explicitly identified in the COE.

Units requesting training will carefully coordinate these opportunities to maximize benefit. If ICS training is being conducted for the AMSC as a precursor to an AMS exercise, potential participants of other upcoming exercises should be included as well. For example, if a PREP exercise is scheduled a year after the AMS exercise, the PREP participants should also be included in the training opportunity. Rotation of personnel or AMSC members should also be considered. The optimal time for training may not necessarily coincide with the delivery of an exercise, but may follow an influx of new or inexperienced personnel.

Contingent upon availability of funds, G-M intends to fund one ICS-320, Intermediate Incident Management Team training (formerly "MATES" (Multi-agency Team Enhancement System)) session per three year cycle of exercises for each FMSC/COTP. Other potential sources of training are listed below.

→ Training Center Yorktown (Tracen Yorktown)

Tracen Yorktown has developed a suite of Incident Command System training programs. Information on the intent of these training programs can be found in the National Incident Management System (NIMS) and National Response Plan (NRP) Implementation Plan which is posted on the Coast Guard Intranet at http://cgweb.comdt.uscg.mil/G-MO/MOR/MOR3/national_response_plan.htm.

→ National Strike Force Coordination Center (NSFCC)

The NSFCC coordinates the activities of the three regional Strike Teams, who in turn can provide specific training and resources in support of exercise conduct.

→ Federal Emergency Management Administration (FEMA)

FEMA maintains web based training for both the National Incident Management System and the National Response Plan through their website at http://www.fema.gov. Both are available at no cost. The FEMA Emergency Management Institute offers an online

course designed to introduce the National Response Plan. It can be found at http://training.fema.gov/EMIWeb/.

5.3. **AMS Exercise Design**

5.3.1. Scope and Participation

The Needs Assessment conducted by the AMSC/FMSC will dictate where attention needs to be focused to improve preparedness, and in turn will dictate specific objectives to be tested in a particular AMS Exercise. Those objectives will then drive the scope of the exercise, as well as the level of participation. The AMS Plan itself is broad in nature; it addresses topics from awareness and prevention to response and recovery. Thus, an AMS exercise may be very comprehensive and broad in scope, or it may be limited to focus on very specific objectives. The following are some key concepts that drive scope and complexity to consider in designing AMS exercises.

5.3.1.1. *Readiness of the AMS Committee and the Port Community*

AMS Exercises will be tailored to the level of sophistication of the AMS Plan as well as the state of the AMSC. If the AMS Plan was recently developed, or significantly updated, and the AMSC has received little training and is not well versed on the Plan, a TTX may be the best option. Once a base has been established, the next progression would be a CPX, then an FSX in successive years. This concept reinforces the training aspect of exercises, and recognizes the value in a progressive approach to build skills and capabilities.

5.3.1.2. *Participation (Industry, Special Response Assets)*

The exercise objectives will determine the appropriate level and type of participation. Port Security incidents or events by their nature involve actions by members of the maritime industry, i.e., facility and vessel owners/operators, among others. It is important for the AMSC/FMSC to consider industry participation in the very early phases of exercise planning, and to gain voluntary participation as appropriate.

Additionally, AMSCs must be mindful of the private sector's requirements for exercising their own security plans. If the AMSC desires industry participation in an AMS Exercise, expectations must be clear in terms of the ability of the exercise to fulfill requirements for testing both the AMS Plan and the industry plan. For instance, vessels and facilities regulated by 33 CFR 104, 105, or 106 hold individual security plans and are required to exercise those plans in accordance with the regulations. The regulations are very specific with regard to facility and vessel security plan (FSP/VSP) exercise requirements. These exercises must involve implementation of the specific vessel/facility security plan, must fully test the security program, and must include substantial and active participation of relevant company, vessel and facility personnel. Thus, an FSO/VSO observing a facilitated discussion tabletop AMS exercise would not be sufficient to meet the FSP/VSP exercise requirement but may meet a facility or ship

quarterly drill requirement, given that elements of their security plan are tested in the AMS exercise.

Participation by specialized entities (such as special teams, National Strike Force, MSSTs, etc.) may also be a factor depending on the scenario. Participation by these types of assets shall be requested through the chain of command. Normally, however, the AMS exercises should focus on local resources. Specialized assets will normally be exercised during regional or national level exercises.

5.3.2. Comprehensive Port Exercises

The concept of a comprehensive port exercise entails the implementation of the AMS Plan as well as several individual vessel/facility security plans in response to a scenario. While high on the complexity scale, such a concept bears consideration as it provides a unique opportunity to truly validate preparedness of the port community as a whole.

5.3.3. Multiple Contingency Exercises

A significant attribute of AMS Plans is that they link to other applicable federal, state, and local response plans with respect to reacting to transportation security incidents. This recognizes that security incidents and/or terrorism events may likely cause secondary impacts (oil spills, hazardous materials releases, mass casualties, etc.) which require specialized contingency response actions along with the implementation of protective security measures. The ability to execute these plans simultaneously and in a coordinated fashion is an important concept that needs to be part of the overall AMS exercise and preparedness program. AMSCs/FMSCs are encouraged to exercise multiple plans/contingencies in this fashion as part of the AMS exercise program on an as needed basis. . In these instances, there must be a critical focus on the exercise planning effort, so as not to have so many objectives that they lose focus or are not fully addressed.

Multiple contingency exercises combining PREP and AMS FSX shall be coordinated between the NSFCC and Area and District Planning Staffs. This shall be done in such a way where the annual requirements for one are combined with the other's three year FSX, on an as needed basis. Contracted AMS exercise support will be integrated with the NSFCC staff support as appropriate to meet the exercise objectives. Multiple contingency exercises that test the AMSP and contingencies other than Oil/ Hazardous Substance spill response, should be coordinated between the appropriate Area and District program managers. When AMS funds are used to support a multi-contingency exercise, the amount shall be proportional to the percentage of AMS Plan play in the exercise.

5.4. **AMS Exercise Objectives**

Listed below are the four Major Objectives and their Supporting Objectives to be used in exercising AMS Plans. Supporting Objectives are listed underneath each Major Objective. The Supporting Objectives lists are not all inclusive. They are intended to provide ideas to exercise planners and to guide but not limit AMSCs in designing AMS Exercises.

AWARENESS: Evaluate the overall maritime situational awareness of the port. Validate risk assessment, and jurisdictional and resource information that underpins security prevention and response planning. Test communication of security related information to include threat information, MARSEC level changes, and MARSEC Directives.

- Test notification process for communicating security information, MARSEC directives, and/or changes in MARSEC Levels to appropriate entities.
- Test communication of security and threat information to Public in non-emergency setting.
- Test communication of security and threat information to Public in emergency setting.
- Test communication of appropriate security and threat information with waterway users (to include Company Security Officers, Vessel Security Officers and Facility Security Officers) in emergency situations.
- Test communication of appropriate security and threat information with waterway users (to include Company Security Officers, Vessel Security Officers and Facility Security Officers) in non- emergency situations
- Test the expected timeframes for responding to changes in MARSEC level, communicating, and tracking attainment.
- Test procedures to inform vessels, facilities, and operations not covered by 33 CFR Parts 104, 105, and 106 of changes in MARSEC Levels.
- Test procedures for addressing situations when entities cannot, or do not, comply with their security plans when a change in MARSEC Level occurs.
- Test procedure for identification of inbound/outbound commercial vessels.
- Validate the role that facilities and shipping agents play as communicators of security information.
- Test procedures used to verify and document receipt of security information.
- Verify list of Facility Security Officers (FSO) located within the COTP Zone, including 24-hr contact information for each FSO.
- Verify list of Company Security Officers (CSO) responsible for the regulated vessels that normally operate at or within its facility, including 24-hr contact information for each CSO.
- Test/verify operational security measures are in place in the port at each MARSEC Level.
- Test procedures for FMSC to conduct spot checks of OPSEC measures (within fours hours of receiving reports of MARSEC Level 2 attainment) employed by vessels and facilities, and vessels and facilities not regulated under 33 CFR Parts 104, 105, and 106, and immediately advise owners/operators of any concerns.
- Test procedures to outline how the FMSC will conduct checks of OPSEC measures (within one hour of receiving reports of MARSEC Level 3 attainment) employed by vessels and

facilities, and vessels and facilities not regulated under 33 CFR Parts 104, 105, and 106, and immediately advise owners/operators of any concerns.
- Test ability to properly handle and safeguard sensitive security information (SSI)

PREVENTION: Test the ability of the FMSC/AMSC/Port Community to effectively implement security procedures, physical security measures, OPSEC measures, and C3 as a result of MARSEC level changes or receipt of threat information. Validate risk mitigation strategies, including assessing the appropriateness and effectiveness of pre-designated preventive and protective security measures. Validate roles, responsibilities, resources and authorities for prevention activities.

- Assess physical security measures and mitigation strategies to be implemented in the port at each MARSEC Level.
- Validate security measures identified to be implemented at the Public Access Facilities at various MARSEC Levels.
- Test the ability to ensure identified security measures at Public Access Facilities are implemented.
- Evaluate procedures for handling reports from the public and the maritime industry regarding suspicious activity.
- Evaluate procedures for handling reports from the public and the maritime industry regarding breaches in security.
- Evaluate procedures that non-105 regulated facilities use to report breaches in security.
- Test/evaluate measures to prevent unauthorized access to designated restricted areas within the port
- Validate roles, responsibilities, authorities, and available resources to implement protective measures at each MARSEC level.
- Evaluate the ability to implement appropriate Operational Security (OPSEC) measures at each MARSEC level. Test procedures to take when a vessel is at a higher security level than the facility or port it is visiting.
- Test procedures to ensure an inbound vessel is instructed to raise its MARSEC Level.
- Test procedures to notify vessels and the FMSC, when a facility receives information that a vessel is arriving operating at a lower MARSEC Level than the facility, and the corrective actions that are taken.
- Evaluate procedures to respond to a report of suspicious activity within the port and the timeframes for such a response.

PREPAREDNESS FOR RESPONSE: Test the ability of the FMSC/AMSC/Port Community to: Respond to suspicious activity, breaches of security, and transportation security incidents (TSI); organize response activities using NIMS and the incident command system; implement linkages with appropriate federal, state, and local response plans; and maintain MARSEC level operations while simultaneously conducting response operations. Validate roles, responsibilities, authorities and resources for response activities.

- Evaluate procedures to report a Transportation Security Incident (TSI), including the contact of the National Response Center and local authorities.

- Evaluate procedures to respond to a report of a suspicious activity or a breach of security within the port and timeframes for such a response.
- Validate most probable TSIs likely to occur in the port AOR.
- Validate linkages to appropriate federal, state, and local response plans in reaction to a TSI.
- Validate and test resources required to respond to a TSI, and who will provide.
- Test the ability and adequacy of resources to conduct simultaneous protective security and response operations.
- Evaluate the ability to establish an appropriate incident command or unified command structure in response to a TSI, including use of the National Incident Management System (NIMS) and participation by appropriate agencies and stakeholders.
- Evaluate/ test links and common objectives between the AMSP and the National Maritime Transportation Security Plan and the National Response Plan.

CRISIS MANAGEMENT AND RECOVERY: Test the ability of the FMSC/AMSC/Port Community to recover maritime transportation system (MTS) functions post-incident. Validate priorities for infrastructure recovery. Validate roles, responsibilities, resources, and authorities for recovery activities.

- Validate priorities for recovery of the MTS post-incident.
- Test procedures for maintaining the integrity of infrastructure post-incident.
- Test/ evaluate procedures to provide post-incident security for facilities not regulated under 33 CFR 105 or 106 but which impact the MTS (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).
- Validate roles, responsibilities, and organizational structures appropriate for post-incident MTS recovery activities.
- Exercise/evaluate procedures and criteria for determining when to reduce the security posture post-incident

6. EVALUATION OF AMS EXERCISES

Developing the Evaluation Plan occurs during the pre-exercise phase, and includes establishing an evaluation team and evaluation criteria for the exercise.

6.1. **The Evaluation Team (Selection of Evaluators)**

The combination and number of people needed to evaluate an AMS exercise will vary depending on the scope and goals of the exercise. In order to provide the AMSC with the perspective vital for an honest assessment, it is anticipated that exercise planners and critical players will not be used as members of the evaluation team.

Non-biased evaluators may be available at the local, District, or Area levels, and do not necessarily need to be members of the Coast Guard. Coast Guard Port Security Specialists and

other members of the field level exercise planning community present good sources for exercise evaluation teams. However, their role in the drafting and execution of the AMSP should be considered in order to determine whether they provide a non-biased approach to the specific exercise and AMSP assessment. While external (to the local port community) evaluation is always recommended, budget and resource constraints may dictate use of local port personnel in these roles. Thus, it is important for AMSCs to identify and/or develop trained evaluators and to look to all available sources for use in evaluating AMS Exercises. DHS, Office of State and Local Government Coordination and Preparedness (OSLGCP)/Office of Domestic Preparedness (ODP), and TSA have experienced exercise evaluators who are available upon request and through notification of the chain of command.

Ideally, personnel selected for AMS exercise evaluation teams should have received certification from an accredited Evaluator Training Course, such as that provided in the Contingency Preparedness Planner and Exercise Planner Course at CG Training Center Yorktown. When this is not the case, personnel determined to be "subject matter experts (SME)" in contingency planning and exercise and evaluation doctrine, as well knowledgeable in the contents, philosophy and purpose of AMSPs, should be identified. The basic guidelines that the AMSC shall follow are:

For AMS Exercises, the Evaluation Coordinator should recruit trained evaluators or SMEs from other AMSCs, from other Coast Guard units such as Districts, Areas, Headquarters, the National Strike Force Coordination Center, or the Incident Management Assistance Team (IMAT), and/or from other federal, state, and local agencies. Members of the local AMSC who would not normally participate in the exercise scenario play may also be used as appropriate. AMSCs/FMSCs shall use the chain of command to request evaluation team members from outside their AOR.

6.2. **Evaluation Criteria**

Specific evaluation criteria for an AMS exercise will be generated during development of the Evaluation Plan, and will be based on specified objectives for the exercise. In order to promote consistency in terms of identifying areas for AMSP improvement, the following eleven evaluation criteria for AMS Plans and Exercises were developed. These general criteria indicate the focus areas to be examined during AMS Exercises. They should be used as a starting point for developing exercise-specific evaluation items.

- Adequacy of operational and physical security measures at each MARSEC level
- Adequacy of Command and Response structure that is consistent with the NIMS requirement established in HSPD-8
- Reasonableness of timeframes (the AMSP provides planning factors which are not performance factors measurable with a stopwatch)
- Adequacy of provisions to maintain infrastructure and operations in the port across MARSEC Levels

- Adequacy of procedures to monitor/verify compliance with CG directives and attainment of MARSEC Levels within the port community
- Adequacy of links to port evacuation and other contingency response plans
- Adequacy of TSI Reporting procedures as well as the response procedures (depending on the type of exercise, (TTX, CPX, FSX) these can range from discussion to deployment of forces/ responders)
- Adequacy of routine and emergency communications within the port community
- Adequacy of information security
- Adequacy of procedures for mandating changes in MARSEC level, designating Special Security Events, Special Security Areas, or Special Security Standards for specific vessels or facilities
- Adequacy of procedures to facilitate recovery of transportation infrastructure after a TSI event

7. **POST-EXERCISE ACTIVITIES**

7.1. **Documentation of AMS Exercises**

The AMSC/FMSC is responsible for completing the exercise After Action Report (AAR) within 60 days of exercise completion. Additionally, the FMSC is required to enter the standard reports into the appropriate CG database (CPS). At this time, Coast Guard exercise planners are not required to enter data into other systems, such as DHS's Lessons Learned Information Sharing (LLIS).

If items in AARs or Lessons Learned (LL) identify security vulnerabilities, it is imperative that such items be designated as sensitive security information (SSI), using the protocols found in NVIC 10-04 and Code of Federal Regulations. For items within AAR/LL that are designated as SSI, they shall be entered into CPS under the SSI category, with the acronym "SSI" put at the beginning and end of the title of the AAR and LL as appropriate. This action will limit access to "covered persons." The SSI distribution limitation statement can be found in NVIC 10-04, Enclosure 3. It must be included in the narrative portion of the AAR/LL as well. Any hard copies of LL/AAR documents containing SSI must also be marked and contain the required limited distribution statements.

Only specific items meeting the SSI criteria shall be designated as such. If there are Lessons Learned that are SSI and some that are not, they will be entered separately into CPS (a SSI category entry and an Unclassified category entry for the same exercise). Multiple entries for a single exercise AAR are acceptable, thus discerning specific SSI Lessons Learned and allowing for the open sharing of information as appropriate.

Once entered into CPS, the AAR/LL will be available for AMSC members or other AMSCs to review through their local CG planners. Specific line items, or the entire set of AAR/LL should be shared with the AMSC, as well as members of the port community in those instances where

plan and process improvement can be achieved. For AAR/LL that are designated as SSI, the CG CPS user is responsible for determining the "covered persons" with a "need to know" and shall ensure SSI information, including that which may be considered proprietary, is not disclosed inappropriately in accordance with the disclosure rules and guidelines found in NVIC 10-04.

7.2. **AMS Plan Amendment Process**

Section 8000 of this NVIC addresses procedures for continuous review and update of AMS Plans. It requires annual review and update, as well as formal review and approval of the Plan every 5 years. The annual review shall be conducted as a precursor to the annual AMS exercise, and updates shall follow the exercise based on findings during the exercise.

Following AMS Exercises, pertinent updates to the AMS Plan shall be completed within 90 days. Items requiring immediate update per Section 8000 will be completed as soon as possible. If *critical areas* of the AMS Plan are updated, the Plan must be submitted to the District and Area for review. *Critical areas* are those defined as such on the Area Maritime Security Plan Checklist which can be found on the CG Internet at http://www.uscg.mil/hq/g-m/mp/mtsa.shtml. The quinquennial District and Area review and approval of plan amendments restart the timeline for the 5 year formal review cycle.

7.3. **Credit for Other Exercises and Real World Events**

CG Area Commanders are responsible for authorizing credit for AMS exercises based on recommendations of the District and the corresponding AMS Committee. The exercises are designed to test the plans, and it is important to assess these newly created plans in a reasonable timeframe. Credit may be sought for exercises or events that occurred after July 1, 2004. Examples of real world events include MARSEC level increases as a result of threat increases, and AMS Plan implementation in response to activities associated with national special security events (NSSE) such as the G8 Summit, national political conventions, etc.

Exercise credit may be granted if the following circumstances exist:

- The AMS Plan was implemented in response to actual threats, real world events, or security exercises conducted with other Federal, State or local agencies. This must involve, at a minimum, significant increase in security planning coordination and activity.
- Appropriate members of the AMS Committee were involved in response to the actual threat, real world event, or security exercise conducted with other Federal, State or local agencies.
- The event/exercise met objectives and minimum standards for assessing the AMS Plan as outlined above.
- The effectiveness of the plan strategies actually implemented were evaluated.

- The response was properly documented. Documentation shall include a cover letter requesting credit submitted via the chain of command that provides the following information:
    - The type of event and exercise the credit requested.
    - Date and time of the event or exercise.
    - Description of the event or exercise.
    - The objectives met in the event or exercise.
    - The sections of the AMS Plan used.
    - Lessons learned, including an AMS Committee analysis of the response compared to activities outlined in the AMS Plan.
    - A statement that the After Action Report and lessons learned were completed in CPS.
    - The sections of the AMS Plan that require improvements, including best practices.
    - Timeline for plan improvements or documentation for immediate corrective actions implemented with approval of the FMSC.
    - Person(s) responsible for updating the AMS plan if critical changes are to be made.
    - Enclosures should include copies of all SITREPS and other incident and/or MARSEC level increase documentation. Units shall be mindful of classification assigned to enclosures and to follow applicable policy for submittal.
    - Documentation must be in writing and signed by the FMSC.

8. **PUBLIC AFFAIRS GUIDANCE**

8.1. **Real Media Coverage of Exercise Events**

Depending on the scale of the exercise, the need for "real" media and public engagement will vary. Providing information that an exercise is being conducted to increase security preparedness is a positive message that showcases our efforts and builds confidence in our security systems. Media coverage should not focus on specific AMS Plan content, items being evaluated, nor vulnerabilities or lessons resulting from the exercise.

For a CPX or TTX, engaging the media for reasons stated above could be beneficial, but is not necessary. For an FTX, engaging the public and the media will be necessary. As a general rule, the more the general public can see or hear during the exercise, the more effort should be placed on fostering positive, well-informed media coverage. Actions could span from a simple press release, to inviting and escorting media to observe exercise play at designated times/locations.

AMSCs/FMSCs shall consult with their District Public Affairs staff to determine the best strategy for media coverage of AMS exercises.

8.2. **Inclusion of Public Affairs in Exercise Play**

Public affairs is also an important part of exercise play. During an actual TSI, high media and public interest is certain. Being prepared to handle this aspect of a TSI will likely have a considerable impact on the perception of the overall success of the operation. The Public Affairs portion of the exercise can include: risk communications training in advance of the exercise, simulated media reports and press releases, and even the stand up of a Joint Information Center. Consult with District and Area Public Affairs staff during planning for input on both "real" and exercise public affairs activities. The NSFCC also maintains Public Information Assistance Team (PIAT) that is available for assistance through the chain of command.

TAB A: FAQs Regarding Expenditure of Exercise Funds

? *Regarding Travel and Per diem, are there limits to the number of planning meetings to develop an exercises or a limit to the number of people required to conduct the exercise [TTX, CPX, FSX] development process?*

→ There is no limit; however, the expectation is that for larger exercises, the number of meetings will be consistent with HSEEP and the standard business practice of an initial, mid-period and final planner's conference.

? *Is hiring Reserves (ADSW) to develop the exercise appropriate? Can Reservists backfill the AD person and we pay that ADSW?*

→ Both are appropriate and acceptable.

? *Regarding ICS Training, is another funding mechanism available thus freeing up money for other aspects of preparedness?*

→ G-MP is working with the National ICS Coordination group to expand both ICS and MATES training to support MTSA exercises as well as PREP exercises. The goal is to have training for each FOSC/FMSC area once every 3 years. Headquarters Program Managers will directly fund the training coordinating with the ICS Coordination group. G-MP will consider other training requests as they are identified, but currently this is the standard ICS training mechanism. Port community participants are not charged a fee for this training but funding cannot be provided for their travel or lodging.

? *Regarding MATES Training, do we pay (directly/indirectly) for port partners to attend training?*

→ See the previous question.

? *What is an appropriate amount to pay a contractor to coordinate a TTX?*

→ According to the current G-MP exercise funding budget model, TTX funding to the unit is set for approximately $10k. For a FTX it is $25k. G-MP is developing a contract vehicle to support hiring of contractors for FTXs (large scale, port community exercises, not internal unit exercises, the planning for which goes well beyond the capability of the individual unit). The contracted services are envisioned to be similar in scope and scale to the PREP Area exercises currently supported by the NSFCC. Contracts are necessary in part because NSFCC does not have the personnel to support further expansion of the exercise support they currently provide. We are developing a contract vehicle and a standard statement of work (SOW) that we would expect the field units to use when contract support services are necessary. That should be in place before FY06. Headquarters will retain all contract money and assist the Local Unit in executing the contract to ensure it is used properly. Recognizing the need for outside support for large scale exercises in FY05, and because the contract vehicle is not yet in place, G-MP has disbursed funds to the Areas, so field units could contract support on their own. For FY05 the oversight burden for contracted assistance with exercises remains with the COTP.

? *Is it acceptable to lease or purchase "preparedness equipment"? Often people ask for poster printers and all in one machine to support an operation.*
→ It is acceptable to request funds to for procuring equipment to conduct an exercise as these items support preparedness.

? *Regarding the leasing of vessels, while typically not cheap, it works for FSXs. How much is too much. Example - $180K to rent a container ship for an international exercise.*
→ If it is deemed appropriate and necessary within budgetary constraints, it would be appropriate to pursue this kind of support. However, such extraordinary expenses should be identified at least a year in advance and guidance and funding support sought from Area and HQ before commitment to such a large investment.

? *Can we pay for external partners training above and beyond ICS? Is it appropriate to use USCG exercise money for training locals on the use of Personal Protective Equipment (PPE), for example?*
→ No, except when such training is appropriate to support CG mission. We can pay for them to attend MATES and ICS because that trains everybody to work together in a unified command. We cannot train non-CG personnel on PPE for example, unless we rely on them as an integral part of a CG team, which is unlikely.

? *Can exercise funding be used to support other regional commands? Groups? Air Stations?*
→ Exercise funds are provided to FMSCs. If an FMSC deems it germane to provide monies to other units in support of overall preparedness, then that is acceptable. There is no expectation that such support would be done routinely.

? *Can this funding be used to host planners and exercisers conferences?*
→ Yes. If it is appropriate to the overall preparedness and support of the unit(s) exercise program(s).

? *What is the Area's obligation in distributing AMSP exercise funds?*
→ Area's obligation is to distribute all funds to the units that are designated for pass through to the units with FMSC responsibility. The unit's obligation is to conduct the full slate of MTSA exercises required of them, to the appropriate scope and scale. Units are expected to maintain a robust exercise program. The money provided may be used in any manner the FMSC deems legitimate to support their AMS exercise program, including support of preparedness activities peripheral to an individual exercise. Areas and Districts are responsible for working together to manage exercise contract and evaluator funds in support of all the units in their AOR.