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

Commandant
United States Coast Guard

US Coast Guard Stop 7618
2703 Martin Luther King Jr Ave SE
Washington, DC 20593-7618
Staff Symbol: CG-FAC
Phone: (202) 372-1080

COMDTPUB P16700.4
April 19, 2019

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 09-02, Change 5

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

Ref: (a) Maritime Transportation Security Act (MTSA) of 2002, Public Law 107-295
(b) Security and Accountability for Every Port Act (SAFE Port Act) of 2006, Public Law 109-347, as amended
(c) Coast Guard Authorization Act of 2010, Public Law 111-281
(d) Magnuson Act of 1950, 46 U.S.C. §§ 70051-70054
(e) Regulations Relating to the Safeguarding of Vessels, Harbors, Ports, and Waterfront Facilities of the United States, Executive Order 10173, as amended
(f) Ports and Waterways Safety Act (PWSA) of 1972, 46 U.S.C. §§ 70001-70036, Public Law 92-340
(g) FAA Reauthorization Act of 2018, Public Law 115-254
(h) Navigation and Navigable Waters, Maritime Security: 33 C.F.R. Parts 101-106
(i) Risk-Based Decision-Making, COMDTINST 16010.3 (series)
(j) Sensitive Security Information (SSI), DHS Management Directive 11056.1 (series)
(k) Sensitive Security Information (SSI) Handling Procedures, Navigation and Vessel Inspection Circular No. 10-04, COMDTPUB P16700.4 (series)
(l) Classified Information Management Program, COMDTINST M5510.23 (series)
(m) Physical Security and Force Protection Program, COMDTINST M5530.1 (series)
(n) Area Maritime Security Plan (AMSP) and Area Maritime Security (AMS) Assessment Development and Maintenance Process, COMDTINST 16601.28 (series)

DISTRIBUTION – SDL No. 169

	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	X	X	X		X									X												
C					X																				X	
D		X		X	X						X															
E					X				X					X				X								
F																										
G																										
H						X																				

NON-STANDARD DISTRIBUTION:

1. PURPOSE. The purpose of this Circular is to: (a) provide guidance to field commanders, the maritime community and Area Maritime Security Committee (AMSC) members on the development and maintenance of Area Maritime Security (AMS) Assessments and Area Maritime Security Plans (AMSPs); (b) provide guidance on the responsibilities of the Captain of the Port (COTP) acting as the Federal Maritime Security Coordinator (FMSC); (c) provide a common template for AMSPs; (d) address port security issues that are the shared responsibility of the port stakeholders and AMSCs, and; (e) promote unity of effort among all stakeholders with maritime security interests at the port level.

2. ACTION. COTPs will give the guidance in this Circular the widest dissemination to the maritime community and AMSC members. COTPs, with the assistance of the AMSCs, should follow the guidance provided in Enclosures (1) through (7) regarding the development of AMS Assessments, and the development, review, exercising, and updating of AMSPs. This Circular will be distributed by electronic means only.

3. DIRECTIVES AFFECTED. NVIC 9-02, Change 4 is cancelled and replaced by NVIC 09-02, change 5. Change 5 provides updated guidance to comply with References (a) through (c). As a result, Enclosures (1) through (7) were revised accordingly. Enclosures (1), (3), (6) and (7) include minor verbiage, grammatical, or formatting updates. Enclosure (2) includes substantial updates to section 3410, 3440, 4340, 4440, 4540, 5400, 5410, 5531, 5532, 5660, 5670, 5680, 6000, 6100, 6200, 6300, 6400, 6500, 9500, 10100, 10300. Enclosure (4) includes substantial updates to "Tab C Exercise Credit Procedures" and the corresponding memo to request exercise credit. Enclosure (5) is a new Cyber Incident Response Template. Enclosure 5 was the previous place holder for the Marine Transportation System (MTS) Recovery Plan/Template. The MTS Recovery Plan/Template was removed from NVIC 09-02 and can be found in NVIC 04-18 titled: "Guidelines for Drafting the Marine Transportation System Recovery Plan." Reference (g) updates are included in Enclosure (2) section 1300(a) and added as a reference to Enclosure (5).

4. BACKGROUND. The MTSA required the Coast Guard to coordinate joint planning for anti-terrorism efforts in the port environment to enhance deterrence and response to Transportation Security Incidents (TSIs) and maritime terrorism threats. The MTSA also required designation of both the geographic areas for which AMSPs were required to be prepared, and a Coast Guard official to serve as the FMSC for each area. AMSPs are required to be integrated with facility and vessel security plans (when required by MTSA), and adequate to deter a TSI when implemented in conjunction with the DHS Transportation Systems Sector-Specific Plan. The SAFE Port Act expanded mandatory content of AMSPs to include a Salvage Response Plan (SRP) to ensure that waterways are cleared, and that commerce through the Nation's ports is reestablished as efficiently and quickly as possible after a maritime TSI. The Coast Guard Authorization Act of 2010 further expanded mandatory content to include area response and recovery protocols to prepare for, respond to, and recover from a TSI. The FAA Reauthorization Act of 2018 will require incorporation of cyber risks into the AMSP in future updates. AMSP content requirements established by 33 C.F.R. Parts 101-103 include the requirements of References (a) through (g), for which maritime community engagement is essential.

5. DISCUSSION.

a. The COTP/FMSCs are responsible for establishing and maintaining AMSCs to provide advice regarding the development and maintenance of an AMSP for each COTP Zone. MTSA-implementing regulations require that each AMSC use a risk-based approach to develop and maintain their AMS Assessment. AMSCs also develop methods to identify port infrastructure and operations, identify risks to the port, communicate threats involving terrorism to affected stakeholders, coordinate resources, and mitigate threats and consequences. Enclosure (1) provides guidelines for the AMSCs.

b. The AMSPs and AMSCs are essential elements of the layered security of our Nation's ports. Collaborative planning, coordination, open lines of communication, strong working relationships, and unity of effort are essential to provide an effective systems approach to preventing, detecting, responding, and recovering from terrorist threats to the Marine Transportation System (MTS).

c. Guidance for the development and maintenance of AMSPs is contained in Enclosure (2) to this document. A standard template for AMSPs is included to assist COTPs/AMSCs in the development of AMSPs, and is designed to meet the regulatory requirements contained in Reference (h).

(1) AMSPs developed by COTPs/AMSCs shall include protocols and procedures for the essential components of the plan, which include; awareness, preparedness, prevention, security response, communications, and recovery coordination and procedures.

(2) The AMSP should also provide for facilitating the recovery of the MTS after a TSI and must include a Salvage Response Plan (SRP) per Reference (b). AMSPs should provide linkages to recovery plans and be compatible across all forms of transportation disruptions, as defined by References (a) and (b), with special attention to MTS recovery and salvage response procedures.

(3) The COTP/FMSC and AMSCs contribute to the Maritime Common Operating Picture (MCOP) by providing decision makers with the situational awareness access to vital information needed to make informed decisions when planning and executing response and recovery operations.

d. AMS Preparedness Stages.

(1) The first stage of the AMSP process begins with an Area Maritime Security (AMS) Assessment of the ports within the COTP Zone. Enclosure (3) describes the process, requirements, and skills needed by personnel to conduct the assessment, and it also discusses the role of the Maritime Security Risk Analysis

Model (MSRAM) in supporting the assessment. Additional information regarding risk-based decision making is available in Reference (i).

(2) The second stage of the preparedness process includes the planning and coordination needed among stakeholders to implement risk reduction strategies identified through the AMS Assessment.

(3) Subsequent stages in the preparedness cycle include exercise, evaluation, After Action Reports (AARs), identification of lessons learned, and AMSP adjustment. Enclosure (4) provides guidance on the AMS Training and Exercise Program (AMSTEP). Recommendations on port security training are also included in Enclosure (4). However, training should be conducted throughout the stages of the preparedness process.

e. AMSPs may contain Sensitive Security Information (SSI). Persons requiring access to a plan that contains SSI must submit a Department of Homeland Security Non-Disclosure Agreement (Tab A to Enclosure 2). Each plan containing SSI is required to be designated and marked as SSI in accordance with Reference (j). Paragraphs will be clearly marked to identify the security designation of information contained in each paragraph (SSI, FOUO, or U). SSI information may be redacted from the AMSP in accordance with Reference (k). However, a redacted plan must also be marked as such in accordance with Reference (k). The redacted AMSP may be shared with the port community consistent with access regulations applicable to its remaining content. Therefore, if a redacted AMSP contains information designated as For Official Use Only (FOUO), then applicable access requirements apply. Additional guidance is provided in References (l) and (m).

f. Protected Critical Infrastructure Information (PCII). PCII, as defined in the Homeland Security Act (6 U.S.C. § 131(3) and § 212(3)), may be important or essential to planning the recovery of maritime Critical Infrastructure/Key Resource (CIKR). Access to PCII will be limited to the purpose for which it was obtained and voluntarily provided by owners of such material. Access to, use of, and safeguarding PCII will be done in strict accordance with the requirements of 6 C.F.R. Part 29. PCII will not be included in the AMSP, and will be maintained and safeguarded separately.

g. AMSP content is derived from specific statutory and regulatory requirements and discretionary authority available to the Coast Guard. AMSPs should not be expanded to include emerging issues without the concurrence of the AMSP program manager in the Office of Port and Facility Compliance (CG-FAC) at Coast Guard Headquarters, in coordination with Coast Guard District and Area Commands. However, emerging initiatives often involve a level of detail or location-specific issues that are more appropriately addressed by COTPs/AMSCs through the development of job aids (e.g., quick response cards and templates for tactical operations), best practices/lessons learned (learned through exercises and training), etc. Such materials may be incorporated by reference in AMSPs where appropriate to AMS content requirements described in Enclosure (2).

6. DISCLAIMER. This guidance is not a substitute for applicable legal requirements, nor is itself a rule. It is not intended to nor does it impose legally binding requirements on any party. It represents the Coast Guard's current thinking on this topic and may assist industry, mariners, the general public, and the Coast Guard, as well as other federal and state regulators, in applying statutory and regulatory requirements. You can use an alternative approach for complying with these requirements if the approach satisfies the requirements of the applicable statutes and regulations. If you want to discuss an alternative approach (you are not required to do so), you may contact Coast Guard Headquarters, Office of Port and Facility Compliance, which is responsible for implementing this guidance.

7. ENVIRONMENTAL ASPECTS/CONCERNS. The development of this NVIC and the general policies contained within it have been thoroughly reviewed by the originating office in conjunction with the Office of Environmental Management, and are categorically excluded (CE) under current USCG CE #33 from further environmental analysis, in accordance with Section 2.B.2. and Figure 2-1 of the National Environmental Policy Act Implementing Procedures and Policy for Considering Environmental Impacts, COMDTINST M16475.1 (series). Because this NVIC contains guidance on, and provisions for, compliance with applicable environmental mandates, Coast Guard categorical exclusion #33 is appropriate.

8. DISTRIBUTION. No paper distribution will be made of this NVIC. An electronic version will be located on the following Commandant web site: http://www.dco.uscg.mil/Our-Organization/NVIC/Year/2000/#2002

9. IMPLEMENTATION.

   a. Coast Guard Area and District Commanders will work with COTPs/FMSCs to establish scalable port security measures based upon input received from the AMSCs. These measures may include Regulated Navigation Areas with a port security component, security zones, or other combinations of regulations issued under 33 C.F.R. Part 165. When implemented, these enhanced port security measures could address security threats within a port area used to deter a TSI. They could also compliment an increased posture needed when Maritime Security (MARSEC) Levels are raised. However, at no time will these security measures prevent a COTP/FMSC from taking more extensive measures, pursuant to existing authority, within their port in times of national emergency or imminent attack.

   b. COTP/FMSC Responsibility.

      (1) Each COTP/FMSC will use the enclosed guidelines to develop and maintain an AMSP and an associated AMS Assessment and exercise program that conforms to the requirements contained in 33 C.F.R. Part 103 and Reference (a). These plans may include State and local Urban Areas Security Initiative (UASI) Emergency Operations Plans, and other geographic sub-plans as annexes as long as the entire COTP Zone is covered. Where a region-wide AMSP has been established and major sub-areas are addressed using AMSC regional

subcommittees, ensure these geographically defined areas are included as annexes to the Plan.

(2) Separate AMSPs may be prepared for individual ports when there are compelling reasons, subject to the concurrence of the AMSP Approving Authority.

(3) COTPs/FMSCs will use the MSRAM as part of the assessment tool to support the development of AMS Assessments as described in Enclosure (3).

(4) Ensure PCII is not contained within the AMSP, and is safeguarded separately.

(5) AMSPs will be submitted by the COTP/FMSC in an electronic format to their District Commander for review in accordance with the Plan Review Authority's direction and Reference (n).

(6) COTP/FMSC will upload approved AMSPs in the appropriate HOMEPORT "Sensitive But Unclassified" community as per Reference (n).

c. District Commander Responsibility.

(1) District Commanders, working with the COTPs/FMSCs, will ensure timelines are met and provide any technical or drafting assistance needed.

(2) District Commanders will review all AMSPs within their District based on the criteria found in Reference (n) and this Circular, and forward the plans to the respective Area Commander for final approval.

d. Area Commander Responsibility. Area Commanders will review and approve all AMSPs in accordance with the criteria found in Reference (n) and this Circular, and inform Commandant (CG-FAC) when approved AMSPs are posted in HOMEPORT.

e. Headquarters Responsibility.

(1) Commandant (CG-5P), the Office of Port and Facility Compliance (CG-FAC), is responsible for policy and guidance governing AMS Assessments and AMSPs, and will coordinate with Commandant (CG-5R), the Office of Contingency Preparedness and Exercise Policy (CG-CPE), to establish and review exercise policy and guidance. CG-FAC is also responsible for policy and guidance governing the oversight of AMSCs and MTS stabilization and recovery policy.

(2) The Office of International and Domestic Port Security (CG-PSA) is responsible for policy and guidance governing the use of the MSRAM, and the Port Security and Resiliency Assessment (PSRA) program.

10. RECORDS MANAGEMENT CONSIDERATIONS. This NVIC has been thoroughly reviewed during the directives clearance process, and it has been determined there are no further records scheduling requirements, in accordance with Federal Records Act, 44 U.S.C. 3101 et seq., NARA requirements, and Information and Life Cycle Management Manual, COMDTINST M5212.12 (series). This non-directive guidance does not have any significant or substantial change to existing records management requirements.

11. FORMS. None.

12. REQUEST FOR CHANGES. Requests for recommended changes to this NVIC should be directed to the Office of Port and Facility Compliance, (CG-FAC-1) at AMSC@uscg.mil.

J. P. Nadeau /s/
Rear Admiral, U.S. Coast Guard
Assistant Commandant for Prevention Policy

Encl: (1) Guidance for Development and Maintenance of Area Maritime Security Committees (AMSC)
(2) Guidance for Development and Maintenance of Area Maritime Security Plans (AMSP)
(3) Area Maritime Security (AMS) Assessment
(4) Area Maritime Security Exercise Program Guidance
(5) Cyber Incident Response Plan Template
(6) Salvage Response Plan Template
(7) Glossary of Terms and Definitions

ENCLOSURE (1) TO NVIC 9-02 CHANGE 5

GUIDANCE FOR DEVELOPMENT AND MAINTENANCE OF
AREA MARITIME SECURITY COMMITTEES (AMSC)

GUIDANCE FOR DEVELOPMENT AND MAINTENANCE OF AREA MARITIME SECURITY COMMITTEES (AMSC)

1. PURPOSE. This enclosure provides information on the purpose, structure, and conduct of AMSCs. It is intended to assist each Captain of the Port (COTP), serving as Federal Maritime Security Coordinator (FMSC), in establishing, maintaining, and directing the AMSCs per 33 C.F.R. § 101.105 and 33 C.F.R. § 103.205.

2. BACKGROUND.

   a. Coast Guard COTPs have established a broad spectrum of port committees, including Port Readiness Committees, Harbor Safety Committees, Area Committees for Oil and Hazardous Substances Response, Heavy Weather Committees, and other Federal, State, and Local committees, to facilitate coordinated response to specific incidents within the maritime domain.

   b. In December 2001, the Commandant of the Coast Guard directed COTPs to establish Port Security Committees (PSCs) in support of the Coast Guard's Homeland Security mission. The Maritime Transportation Security Act of 2002 (MTSA) (P.L. 107-295) authorized the Secretary of the department in which the Coast Guard is operating to establish Area Maritime Security Advisory Committees. Pursuant to MTSA authority, the Coast Guard issued regulations for Area Maritime Security in 33 C.F.R. Part 103. The regulations also implemented a change in terminology from "Port Security" to "Area Maritime Security" for both plans and committees, and defined Area Maritime Security Committee (AMSC) to mean the committee established pursuant to 46 U.S.C. § 70112(a)(2)(A).

   c. MTSA specifically waives the application of the Federal Advisory Committee Act (FACA), 5 U.S.C. App. Sec. 14, for AMSCs. Each AMSC is required to conform to certain provisions in MTSA, and the procedures established in 33 C.F.R. § 103.300. In particular, MTSA establishes minimum requirements for committee composition, member experience, solicitation of nominations, and provides authority for passing a security background examination prior to appointment as a member. Additionally, 33 C.F.R. § 103.300 mandates a written charter for the formation of AMSCs.

3. DISCUSSION.

   a. Establishment of AMSCs. The AMSC program supports the Coast Guard's Ports, Waterways, and Coastal Security (PWCS) mission through interagency, intergovernmental, and public/private sector cooperative efforts. As the Lead Federal Agency for Maritime Security, the Coast Guard will accomplish the PWCS mission, in part, through AMSCs that provide a framework to identify

risks to the port, communicate information regarding threats to port stakeholders, and determine mitigation strategies and implementation methods.

b. Purpose and Responsibilities of the AMSCs.

(1) The purpose of the AMSC as specified by 33 C.F.R. § 103.300 is to assist and advise the COTP regarding the development, review, and updating of an Area Maritime Security Plan (AMSP) for its Area of Responsibility (AOR) that addresses attacks upon the particular infrastructure within each COTP Zone that would most likely create a Transportation Security Incident (TSI). In doing so, the AMSC should reference the definition of infrastructure in 33 C.F.R. 101.105. The MTS initiative to safeguard infrastructure evolved from "An Assessment of the U. S. Marine Transportation System," (U.S. DOT, 1999).

(a) The AMSCs support development of the AMSP and maritime security preparedness by serving as a link for security awareness, ensuring that an AMS Assessment and written report of AMS Assessment are completed as required by 33 C.F.R. § 103.400, and participating in the exercising of AMSP elements. They assist the COTP in correlating AMS activities and maritime security preparedness with Presidential Policy Directive 8 (PPD-8), National Preparedness, and its protection, mitigation, and response frameworks.

(b) The AMSCs support implementation of the AMSP by serving as a link for communicating threats and changes in MARSEC Levels.

(c) The AMSCs provide technical support for evaluation of Port Security Grant proposals in support of AMSPs.

(2) The AMSCs support the information-sharing framework consistent with Homeland Security requirements and direction, including in part, the National Infrastructure Protection Plan (NIPP) (plan maintained by the Cybersecurity and Infrastructure Security Agency (CISA)). AMSCs should use Alert Warning System (AWS) to disseminate critical information, and use HOMEPORT, the Coast Guard's public internet portal, to improve communication and information sharing. AMSCs should encourage the use of similar programs to raise the security awareness of port community stakeholders and encourage threat reporting through the National Response Center (1-800-424-8802). For immediate danger to life or property call 911, or call the Coast Guard on Marine VHF-FM Channel 16. AMSCs are directed in 33 C.F.R. § 103.310 to act as a link in communicating threats to maritime security to stakeholders, and changes in MARSEC levels. This regulation was designed to address concerns voiced by industry and the boating public regarding the

communication of threat information and protection of propriety or other private information. The Communications Section of the AMSP Template in Enclosure (2) section 3400 to NVIC 9-02 (series) is intended to serve as a guide to the COTPs/FMSCs in the development of communications plans that address those concerns, and in identifying the role of the AMSC in the communications process.

(3) The PWCS mission encompasses national security objectives pertaining to the MTS, including the need to support military operations conducted in port areas by the Department of Defense (DoD). The AMSC advises the COTP on the development of security plans and procedures for the COTP Zone. Although the AMSC is not a response entity for the purposes of crisis management, it may be asked to provide subject matter expertise to advise the COTP/FMSC. The links between the AMSC and response organizations such as Local Emergency Planning Committees (LEPC), Area Committees for Oil and Hazardous Substances Response and other existing port committees are crucial to improving overall preparedness and resiliency. Just as jurisdictions in the ports are overlapping, some committee responsibilities may overlap. The need for coordination in the designated Strategic Commercial and Strategic Military Seaports has been directly addressed by the Port Readiness Committees (PRCs) and the National Port Readiness Network (NPRN).

c. AMSC Area of Responsibility (AOR). The AMS program standard is one AMSC (and one AMSP) for each COTP Zone. The AMSC serves under the direction of the respective COTP/FMSC within each respective COTP Zone as summarized below. Specific details are found in Enclosure (2) to NVIC 9-02 (series).

(1) Subject to Coast Guard Area Commander approval, the geographic area within a COTP Zone may be subdivided to facilitate program administration and AMSP development (e.g., Guam and Commonwealth of Northern Marianas, Gulf of Mexico [GOM]). An AMSC (and AMSP) will be established for each such AMS area.

(2) For COTP Zones that cover large geographical areas (e.g., Western Rivers COTP Zones), the COTP/FMSC may establish AMSC regional sub-committees to facilitate stakeholder engagement for those sub-regions and identified in the respective AMSP. The AMSC regional sub-committees must be provided for, and operate under, the structures and procedures content of the written charter for the parent AMSC. The procedures may include a subordinate written charter for regional subcommittees with content comparable to the AMSC written charter. The AMSP should be used to document the use of regional sub-committees within a COTP Zone, and include a geographical AMSP

Annex to address AMS measures where established for those port areas with AMSC regional subcommittees.

d. Committee Composition Requirements.

(1) Pursuant to MTSA, an AMSC must consist of not less than seven members, each of whom must have at least five years of practical experience in maritime security operations. Pursuant to the Coast Guard Authorization Act of 2010, AMSC composition must include individuals who represent the interests of the port industry, terminal, operators, port labor organizations, and other users of port areas.

(2) 33 C.F.R. § 103.305 specifies that AMSC membership will consist of persons who have an interest in the security of the area, and may be selected from a broad cross section of stakeholder categories. These categories provide balance and depth of coverage for essential expertise consistent with AMSC enabling authorities.

(3) Pursuant to MTSA and the Coast Guard Authorization Act of 2010, appointed members serve as individuals and represent the interests of their stakeholder segment in performing official AMSC duties.

e. Organization of AMSCs.

(1) Committee Organization. When soliciting individuals to serve as appointed AMSC members, the COTPs/FMSCs will take into account all aspects of the MTS in each port area and its adjacent waterways, coastal/shore-side areas and river systems that are under Coast Guard jurisdiction, in order to minimize maritime security risks to each COTP Zone.

(a) Broad representation is necessary to encourage and provide for the AMS Area-wide, public-private maritime security partnership envisioned by MTSA. In order to achieve this objective without imposing excessive burden on available Coast Guard and stakeholder resources, AMSCs may be organized to include appointed members, designated federal agency observers pursuant to MTSA, and other participants serving in an unofficial capacity authorized by the COTP.

(b) The official AMSC roles and responsibilities for AMSC members are specified by 33 C.F.R. § 101 et. seq., and are vested exclusively in, and remain the responsibility of, the appointed AMSC members.

(c) Administratively, an AMSC may be organized into a steering body (e.g., Steering Committee, Managing Board) and a stakeholder-supplemented committee, which accommodates other participants authorized by the COTP.

(2) AMSC Membership. AMSCs consist of members appointed under 33 C.F.R. § 103.305. The COTP may allow participation in the AMSC and its activities by observers from other government agencies, and by other authorized participants, consistent with provisions of each specific AMSC's written charter. These other participants may be referred to as "associate" members, or alternately, as "at-large" or "general" members per existing practice in some AMSCs.

(a) Appointed Members. The official AMSC for fulfillment of regulatory duties consists of members who are appointed by the COTP/FMSC. AMSC appointed members serve their AMSC regulatory duties as individuals representing their area of expertise or maritime industry segment. Appointed members may distinguish between their AMSC regulatory responsibilities and an entity with which they are affiliated, and separately represent the views of the latter.

(b) Federal Agency Observers. The COTP is authorized and encouraged to invite participation in AMSC activities by observers from other Federal agencies to represent each agency's maritime security interests. In this regard, the Coast Guard works closely with the U.S. Army Corps of Engineers (USACE) to ensure a coordinated approach to maintaining the functionality and safety of the nation's ports and waterways navigation systems. The COTP will work closely with USACE Districts to encourage an appropriate level of participation in AMSC activities to enable USACE connectivity and involvement for pre-planning and integration during all-hazards responses.

(c) Other Authorized Participants. The COTP, in consultation with appointed AMSC members, is authorized to supplement the committee by offering participation to stakeholder representatives that qualify for access to sensitive but unclassified maritime security information and activities. Other authorized participant access and participation must be provided for in the AMSC's written charter and conform to all applicable requirements, procedures and protocols for AMSC activities. Other authorized participants may assist the AMSC individually or as a representative of the organization with which they are affiliated, and may include, but are not limited to, subject matter experts whose input is necessary in the development of the AMSP and other activities. At the discretion of

the COTP, these individuals may participate in the activities of the AMSC, sub-committees, and/or working groups.

(3) Partner and Stakeholder Representation. The AMSCs should be representative of federal, state, tribal, territorial and local agencies; marine industry; and other port stakeholders. Representatives for each aspect of the MTS and those charged with its regulation or enforcement should be encouraged to participate. For example, AMSC appointed membership, agency observers, and other authorized participants could include, but should not be limited to, representatives from the following:

(a) Federal Agencies:

- U.S. Coast Guard (e.g., Sectors, Vessel Traffic Service, Maritime Safety and Security Teams, Coast Guard Auxiliary);
- Department of Defense (DOD);
- Nuclear Regulatory Commission (NRC);
- US Department of Agriculture (USDA);
- Environmental Protection Agency (EPA);
- Occupational Safety and Health Administration (OSHA);
- Federal Bureau of Investigation (FBI);
- Federal Emergency Management Agency (FEMA);
- Bureau of Customs and Border Protection (CBP);
- Bureau of Immigration and Customs Enforcement (ICE);
- Transportation Security Administration (TSA);
- U.S. Army Corps of Engineers (USACE);
- U.S. Transportation Command (USTRANSCOM);
- Military Sealift Command (MSC);

- Military Surface Deployment and Distribution Command (SDDC);
- Animal and Plant Health Inspection Service (APHIS);
- Maritime Administration (MARAD);
- Pipeline and Hazardous Materials Safety Administration (PHMSA);
- Federal Railroad Administration (FRA);
- Federal Highway Administration (FHWA);
- Federal Transit Administration (FTA);
- Other government representatives, where appropriate.

(b) State and Local Agencies:

- National Guard;
- Police;
- Fire Departments;
- Civil Defense;
- Transportation agencies;
- Fish and wildlife marine units;
- Health agencies;
- Occupational safety agencies;
- Terminal/facility security forces;
- Other state and local government representatives;
- State and local environmental agencies and marine units;

- Regional development agencies/metropolitan planning organizations.

(c) Tribal Governments:

(d) Territorial Governments:

(e) Industry-related Components:

- Vessel Agents;
- Cargo Owners;
- Facility owners/operators;
- Terminal owners/operators;
- Company Facility Operations Technology Specialist;
- Chief Security Information Officers;
- Trade organizations;
- Railroad companies;
- Trucking companies;
- Shipyards;
- Towing vessel operators;
- Marine exchanges;
- Industry organizations;
- Marine Pilots;
- Organized labor;
- Commercial fishing industry;

- Waterborne vendors & service providers (harbor tugs, launch services, line handlers, small ferry operators, water taxis).

(f) Other Port and Marine Partners:

- Recreational boating organizations (yacht clubs, rowing clubs);
- Associations representing maritime interests, including, but not limited to, National Association of State Boating Law Administrator (NASBLA) members;
- Private and commercial sport fishing groups.

f. AMSC Appointment Process. Appointment of an individual to serve on the AMSC first requires publication of a notice in the Federal Register soliciting nominations for membership.

(1) MTSA, at 46 U.S.C.A. § 70112(b)(3), requires that a notice soliciting nominations for AMSC membership will be published in the Federal Register before appointing a member to an AMSC. The COTP is likely to be the first to know of pending local AMSC vacancies. Experience has shown that vacancies will likely occur more frequently than every 3, 4, or 5 years. Accordingly, a more practical approach to managing AMSC vacancies is for each COTP/FMSC to promulgate solicitations for AMSC membership when needed, rather than Coast Guard Headquarters promulgating a consolidated notice. A sample template Federal Register Notice for use by the COTP/FMSC in promulgating a solicitation notice is included as Tab A of this Enclosure.

(2) Subsequent to the solicitation/application process, a COTP/FMSC may become aware of other individuals or sectors of the port industry or other stakeholders that he/she believes should be represented in the AMSC. The COTP/FMSC may 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 as observers or other authorized participants outside the Federal Register process to ensure strong agency representation on an AMSC. Also, for those members who may have already been designated in writing by the COTP/FMSC as appointed members of an AMSC, it is not necessary for these members to reapply for their positions.

(3) 33 C.F.R. § 103.305(b) requires that at least seven of the members of each AMSC have five years of experience related to maritime or port security operations within the area. The COTP/FMSC will use his/her best

judgment in selecting individuals that are best suited as members of the AMSC, and in determining if each member's qualifications meet the intent of the regulations.

(4) In accordance with 33 C.F.R. § 103.305, each member of the AMSC will be appointed for a term of not more than five years. The COTP/FMSC will designate membership terms to ensure that the terms of appointed members do not all expire within the same year. As such, when establishing an AMSC, some members may be designated for only three years, vice five, to provide for continuity of AMSC service and support. Appointment as an AMSC member will be made in a formal written document. The COTP may reappoint AMSC members for additional terms. Sample Invitation, Appointment and Acceptance letters are provided as Tabs B, C, and D.

(5) At the discretion of the COTP/FMSC, non-U.S. citizens may serve as AMSC members or participate as observers or subject matter experts if they are representatives of foreign governments or lawful permanent residents of the United States. All foreign disclosure restrictions on the sharing of classified information and Sensitive Security Information (SSI), including the TSA terrorist screening check described in paragraph 3(i) of this section apply.

(6) Each AMSC 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. Because the AMSC is established and maintained under the COTP's direction, the COTP/FMSC may chair the AMSC. Nevertheless, some ports may find that under their existing committee structure it is more effective for industry representatives to chair the AMSC. Either method of chairing the AMSC is acceptable under the provisions of 33 C.F.R. Part 103.

(7) The COTP/FMSC will designate a member of his/her staff as the AMSC Executive Secretary of the AMSC. The Executive Secretary will be responsible for the administrative duties of the AMSC, such as maintaining current designation letters, publishing meeting agendas, recording meeting minutes, and maintaining current editions of the AMSP, including digital versions on its Homeport AMSC Community (SBU). It is also the responsibility of the Executive Secretary to ensure that all committee records are properly safeguarded and maintained in accordance with the Classified Information Management Program, COMDTINST M5510.23 (series) and designated as SSI where appropriate. It is also the responsibility of the Executive Secretary to ensure that all committee records are properly safeguarded and maintained in accordance with the Information and Life Cycle

Management manual, COMDTINST M5212.12 (series). It is the general practice of many units to designate a civilian Port Security Specialist (PSS) as the Executive Secretary.

g. AMSC Compensation.

(1) 46 U.S.C. § 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 AMSCs and the National Maritime Security Advisory Committee (NMSAC)) is entitled to receive compensation and travel or transportation expenses. This section does not authorize compensation and travel or transportation expenses for other authorized participants.

(2) The Commandant has determined that compensation for participation on AMSCs will be set at $0. For travel and transportation costs, the Coast Guard has determined that a rate of $1 will apply to appointed members of AMSCs because the AMSCs will meet locally. The COTP may include a statement in the AMSC charter stating that members will forego reimbursement for transportation, travel and compensation expenses costs associated with participation on the AMSC, and require all members to sign the charter to acknowledge the waiver of travel fees and compensation.

(3) If the COTP/FMSC determines that, due to unusual circumstances, it is necessary to pay travel for designated AMSC members, the COTP/FMSC may authorize travel expenses from within the COTP's operating budget.

h. AMSC Meeting Frequency.

(1) Each AMSC will meet at least once during a calendar year, or when requested by a majority of the AMSC members in accordance with 33 C.F.R. § 103.300(b) (4). More frequent meetings are encouraged (e.g., quarterly meetings) in support of maritime domain awareness, and to maintain currency of points of contact and coordinating relationships.

(2) COTPs should take advantage of telephone and video conferencing when in-person meetings are impractical.

i. Information Security.

(1) Sensitive Security Information.

(a) Much of the work of the AMSC will involve handling Sensitive Security Information (SSI). Once developed, the AMSP will contain

SSI material and will be marked and handled in accordance with Guidelines for Handling Sensitive Security Information (NVIC 10-04).

(b) The COTP/FMSC, in conjunction with the AMSC, is responsible for developing procedures to protect both SSI and classified information that is developed and used by the Committee. Once portions of the AMSP or its annexes are designated as SSI, each paragraph will be marked according to the type of information contained therein (e.g., U, SSI, or FOUO). These paragraph markings will aid the COTP/FMSC should it become necessary to redact SSI information to broadly share with the port community the portions of the AMSP that are not SSI. If the COTP/FMSC needs to release safeguarded (i.e., non-SSI or FOUO) portions of the AMSP, the COTP/FMSC will ensure that the redacted AMSP information is marked as having been redacted following procedures provided in NVIC 10-04.

(c) 33 C.F.R. § 103.305(c) grants the Coast Guard authority to request a TSA name-based terrorist check on all AMSC members if it is determined by the COTP that they will need access to SSI. FMSCs will provide the information required for name-based terrorist checks to TSA via Coast Guard Headquarters (instructions in PSS Resource Folder). The TSA name-based terrorist check is required unless the member possesses a federally issued security clearance, is a credentialed federal, state, tribal, territorial, or local official, holds a valid Transportation Worker Identification Credential (TWIC), or has passed a comparable security threat assessment. All new AMSC members needing a name-based terrorist check will be screened against the terrorist watch list prior to having access to SSI. All AMSC members currently having access to SSI will continue to have access while the name-based terrorist check is being performed. If a COTP has not received written notification that an AMSC member is barred from access to SSI after 30 days from submitting their name, the COTP may assume that any name submitted was cleared and is acceptable for the purposes of access to SSI. In addition, the COTP must determine that, prior to discussing or distributing SSI with AMSC members, those members are "Covered Persons" with a "need to know," and have signed a Non-Disclosure Agreement (NDA) as described in NVIC 10-04. The AMSC Executive Secretary will retain the original, signed NDA until the information requiring the execution of the NDA is no longer considered SSI.

(d) The MTSA explicitly states in 46 U.S.C. § 70103 (f) 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 C.F.R. Parts 104, 105, and 106 for COTP Zones that are under the control of the COTP are designated as SSI, and restricted from public access.

(e) General information dealing with the port or infrastructure topics should be made available to all members of the AMSC with a "need to know." However, COTPs 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, AMSC 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.

(f) AMSC 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, COTPs will ensure that all material designated as SSI, and all records of discussions of material designated as SSI, are protected from disclosure to the public, in accordance with NVIC 10-04.

(2) Classified Information.

(a) It is not anticipated that AMSCs or AMSPs will regularly discuss or contain classified information. Classified materials incorporated into the AMSP should be prepared as separate documents, referenced in the unclassified plan, and handled and stored in accordance with proper security procedures outlined in the Classified Information Management Program, COMDTINST M5510.23 (series).

(b) However, if the need arises to discuss classified information with members of the AMSC, the COTP may request security clearances for those AMSC members with whom the COTP intends to share the information. The Coast Guard is permitted to sponsor and grant clearances of AMSC members upon approval of the local Command Security Officer (CSO) and after sending a request to program for authorization to proceed with the process. Specific procedures are found in Chapter 6 of the Personnel Security and Suitability Program Manual (COMDTINST M5520.12 (series)).

j. Templates. Tabs (A) through (D) of this Enclosure contain templates for Federal Register Notices and letters required as part of the process to appoint persons to AMSCs.

TAB A: Federal Register Sample Notice Template

FEDERAL REGISTER NOTICE

DEPARTMENT OF HOMELAND SECURITY 4910-15-U

Coast Guard

[DISTRICT DOCKET NUMBER]

Area Maritime Security Advisory Committee (AMSC) *[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 AMSC (AMSC) *[NAME OF PORT]* submit their applications for membership to the Captain of the Port (COTP) *[NAME OF PORT]*.

DATES: Requests for membership should reach the U.S. Coast Guard COTP *[NAME OF PORT] [DATE, which is 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 at the following address: *[INSERT ADDRESS]*.

FOR FURTHER INFORMATION CONTACT: For questions about submitting an application or about the AMSC in general, contact *[NAME OF A PERSON]*, *[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 Advisory Committees for any port area of the United States. (See 33 U.S.C. 1226; 46 U.S.C. 70112; 33 C.F.R. § 1.05-1, 6.01; Department of Homeland Security Delegation No. 0170.1). The MTSA includes a provision exempting these AMSCs from the Federal Advisory Committee Act (FACA), Public Law 92-436, 86 Stat. 470 (5 U.S.C. App.2). The AMSCs shall assist the Captain of the Port 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 strategies to facilitate the recovery of the MTS after a Transportation Security Incident; 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 in developing and maintaining the Area Maritime Security Plan.

AMSC Membership:

Members of the AMSC should have at least five years of experience related to maritime or port security operations. The *[NAME OF PORT]* AMSC has *[NUMBER]* members. We are seeking to fill *[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 five years; however, a member is eligible to serve additional terms of office. Members will not receive any salary or other compensation for their service on an AMSC. In support of the USCG policy 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 Captain of the Port, 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: *[DATE]*.

_____

[NAME OF COTP/FMSC]
Captain, U.S. Coast Guard,
Captain of the Port/Federal Maritime Security Coordinator *[CITY NAME]*

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

[COTP]
United States Coast Guard

[STREET ADDRESS]
[LOCATION, STATE]
Staff Symbol:
Phone: (000) 000-0000
Fax: (000) 000-0000

16601

Tab B: AMSC Invitation Letter Template

Dear *[RECIPIENT]*:

It is a great pleasure to invite you to serve as an appointed member on the Area Maritime Security Committee (AMSC) for *[NAME OF AMSC]* Committee. 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. Your service will be performed as an individual representing your area of expertise or maritime industry segment when performing duties specified by regulation for appointed members, and that others may not be deputized to attend meetings in your place.

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 AMSCs, and which will provide the foundation for the *[NAME OF AMSC]* upon which you will serve if you accept the appointment.

By accepting the appointment, you will be committee 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 AMSC]* Committee. If you choose to accept this invitation, your appointment to the *[NAME OF AMSC]* Committee will be for *[NUMBER]* 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 OF AMSC]* 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 Area Maritime Security Committee in the immediate future.

Sincerely,

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

Enclosure: Acceptance of Appointment Letter

Copy: *[NAME OF AMSC]* Committee
Commander, *[SPELL DISTRICT NUMBER***]** Coast Guard District (*[#]*)

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

[COTP]
United States Coast Guard

[STREET ADDRESS]
[LOCATION, STATE]
Staff Symbol:
Phone: (000) 000-0000
Fax: (000) 000-0000

16601

Tab C: AMSC Appointment Letter Template

Dear *[RECIPIENT]*:

It is my pleasure to appoint you as a member of the Area Maritime Security Committee (AMSC) for *[NAME OF AMSC]* Committee. This appointment is effective *[DATE]* and shall expire on *[DATE]*.

I have enclosed a copy of the *[NAME OF AMSC]* 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 *[NAME OF PERSON]* of my staff at your earliest convenience regarding the upcoming schedule of *[NAME OF AMSC]* Committee 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
Captain of the Port, _____
Federal Maritime Security Coordinator

Enclosure: Committee Charter

Copy: *[NAME OF AMSC]* Committee Chair
Commander, *[SPELLED DISTRICT NUMBER***]** Coast Guard District (*[#]*)

Tab D: Acceptance Letter Template

Acceptance of Appointment

to the

_____ Committee

I hereby accept an appointment to serve on the _____ Committee, for period to be designated by the Coast Guard Captain of the Port, as 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 my service is as a representative of an area of expertise or maritime industry segment, and that I am not authorized to deputize others to attend meetings in my place. I further understand that the Coast Guard Captain of the Port 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 Name

ENCLOSURE (2) TO NVIC 9-02 CHANGE 5

GUIDANCE FOR DEVELOPMENT AND MAINTENANCE OF AREA MARITIME SECURITY PLANS (AMSP)

GUIDANCE FOR DEVELOPMENT AND MAINTENANCE OF THE AREA MARITIME SECURITY PLAN (AMSP)

1. PURPOSE.

   a. This enclosure provides guidance to the Captain of the Port (COTP) on the preparation and maintenance of the Area Maritime Security Plan (AMSP). The Area Maritime Security Committee (AMSC) is charged with advising the COTP on maritime security matters, and assisting with the development and continual review and maintenance of the AMSP. The AMSC's input is considered vital to the planning process as the Coast Guard seeks to build on Area Maritime Security (AMS) Assessments to develop deterrence, protection, security response and recovery strategies, protocols and procedures for Transportation Security Incidents (TSI) and security threats that may cause a heightened level of security in our Nation's ports and coastal waterways.

2. BACKGROUND.

   a. 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 Marine Transportation System (MTS) from TSIs. Therefore, it is essential that DHS, other federal, state, tribal, territorial, and local agencies, and private industry voluntarily contribute resources to assist with the development and maintenance of the AMSP and support of first responder activities within the maritime domain.

   b. The first step in developing and maintaining the AMSP is completing or revalidating an Area Maritime Security Assessment. The most current and valid port and facility data should be entered into the Maritime Security Risk Analysis Model (MSRAM), which then uses the data to calculate relative risk based on the Coast Guard Risk-Based Decision Making (RBDM) methodology (using a "Threat X Vulnerability X Consequence" algorithm). Each of the components of the formula is broken down into multiple benchmarks with weighted numerical values. The MSRAM analysis results in a scenario-based Risk Index Number (RIN) that can be used to formulate the ranking of assets within a port or jurisdiction, and support the development or updating of AMS Assessments as required by 33 C.F.R. § 101.510, § 103.400, § 103.410, and § 103.510.

   c. Each AMSC should review and incorporate the most current MSRAM data and other relevant assessments (e.g., Threat and Hazard Identification and Risk Assessment, Port Security Resiliency Assessment (PSRA), etc.) as part of the AMSP and AMS Assessments development process. Building upon these nationally focused assessments; the Area Maritime Security Assessment for a particular COTP Zone should maintain a local emphasis and focus on priorities set by port stakeholders. Each COTP/ FMSC should consider the most current

MSRAM data, associated risk analysis, available intelligence assessments, and critical infrastructure risk profiles (e.g., facilities, vessels, etc.) when developing TSI scenarios and strategies for employing resources within the COTP Zone. The annual MSRAM data revalidation cycle and resulting analysis will facilitate adjusting the AMSP based on changing security needs and threats.

d. The primary composition of the AMSP centers on a tiered planning structure based on the Maritime Security (MARSEC) Levels. The AMSP must include strategies for port operations at each MARSEC Level, including pre-determined security protocols and measures to be implemented at each MARSEC level by the Coast Guard, other port stakeholders, and by facilities and vessels subject to provisions of 33 C.F.R. Parts 101-106. Security measures may include deployment of a variety of security and response teams such as armed Coast Guard vessels, boarding teams, and Coast Guard Maritime Safety and Security Teams as appropriate to the MARSEC level and local threat/risk conditions. Security measures may also include the deployment of additional federal, state, or local law enforcement agencies. The use of security regimes are part of the layered security strategy in ports, including the implementation of Regulated Navigation Areas, Security Zones, Marine Events of National Significant (MENS), National Special Security Event (NSSE), Naval Vessel Protection Zones, and U.S. Army Corps of Engineers (USACE) Restricted Areas.

e. The Maritime Transportation Security Act of 2002 (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 of facilities in 33 C.F.R. § 101.105 was carried forward in 33 C.F.R. Part 105 for the purpose of regulating those facilities determined by the Secretary of DHS most likely to be involved in a TSI (excluding Department of Defense facilities). For facilities within the 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 this evaluation should be reflected in the AMSP, with appropriate information regarding facility vulnerabilities shared with the AMSC and affected facility owners/operators.

f. MTSA does not provide COTPs with the authority to impose additional security requirements on vessels or facilities.

(1) Implementation of the MTSA and SAFE Port Act through 33 C.F.R. Parts 101-106, 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.

(2) If the COTP determines it necessary to impose additional requirements on vessels or facilities in the COTP Zone, the COTP may do so only if the authority arises pursuant to either the Magnuson Act or the Ports and Waterways Safety Act (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.

g. COTPs/FMSCs, in collaboration with the AMSCs, will identify the security protocols and measures to be included in the AMSP. COTPs/FMSCs and the AMSCs should coordinate with other federal, state, tribal, territorial, and local agencies that have developed security standards for other critical infrastructure identified in the Area Maritime Security Assessment.

h. COTPs/FMSCs, in collaboration with the AMSCs, will identify protocols and measures by reference to be implemented to facilitate recovery of the MTS as specified in section 6200 of this plan, including salvage response following a TSI, or the threat thereof. COTPs/FMSCs and the AMSC should coordinate with other federal, state, tribal, territorial, and local agencies that have also developed recovery standards and procedures for other critical infrastructure identified in the AMS Assessment.

i. The final stage in the preparedness cycle is the training, exercising and evaluation phase. 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. The exercise phase, in conjunction with plan development, provides means to develop and build cooperative, mutually supporting maritime security and MTS recovery relationships.

3. DISCUSSION.

a. The AMSP developed by the COTP/FMSC and the AMSC must address the maritime domain within the entire COTP Zone, but the COTP/FMSC has discretion on how to present the geographic area(s) covered within the Plan, subject to the concurrence of the Plan Approving Authority. This flexibility is necessary since different geographic areas within the COTP/FMSC Zone may have significantly disparate security concerns and protection strategies. In those cases, the COTP/FMSC may elect to complete the template provided in this enclosure for each geographic region within the COTP Zone. If the COTP/FMSC prepares multiple geographic plans, the standard template and numbering system will still apply, and multiple geographic plans will be brought under the cover of a single base AMSP. Conversely, in some cases there may be a need for a distinctly separate plan for a portion of the area, for example, to reflect a significantly different local stakeholder composition.

Some COTPs/FMSCs may also determine that certain areas within the COTP Zone have such similar security concerns and protection strategies to merit combining the different areas under one base AMSP. Where a region-wide AMSP has been established and major sub-areas are addressed using AMSC regional sub-committees in geographic plans, the COTP/FMSC will ensure those geographically defined areas are included as Annexes within the base AMSP.

b. The AMSP is a communication and coordination tool for the port community. Therefore, certain sections of the Plan must remain available to all law enforcement and port agencies with port security responsibilities. Accordingly, COTPs/FMSCs and AMSCs must remain cognizant of the methods by which Sensitive Security Information (SSI) and other sensitive but unclassified information in the Plan will be protected from unauthorized or unnecessary disclosure.

c. The AMSP Template establishes a standard format for the development of the AMSP, and is intended to assist COTPs/FMSCs in ensuring that all applicable requirements of the MTSA, SAFE Port Act, and the Coast Guard Authorization Act of 2010 are satisfactorily addressed. Guidance is provided throughout the template to assist in the development of the Plan. Bracketed text in small capitals within the template indicates the information that should be provided in each section. Text shown in *italics* is suggested narrative for inclusion in the Plan.

Where AMSC Regional Subcommittees are established, an AMSP (Base Plan) with AMSP port-specific Annexes may be a better option for COTP/FMSCs to consider using. AMSP Annexes established under AMSC Regional Subcommittees help address maritime security measures for those port areas within large geographic or complex COTP Zones instead of capturing all Plan elements in the standard "one-plan" concept. AMSP Annexes can produce significant benefits by: raising the level of importance to those port areas with an established AMSC Regional Subcommittee; assisting the COTP/FMSC and AMSC Regional Subcommittee with review and prioritization of Port Security Grant Program projects within that specific port area; and with planning of port-specific AMSTEP exercises. A sample AMSP Base Plan template and an AMSP port-specific Annex template can be obtained from the AMSP Plan Approval Authority by request.

(1) COTPs/FMSCs should consider the discretionary use of appendices as addendums to the Plan. Appendices provide flexibility in plan development, and should be used to help separate relevant information within the plan such as SSI-related information.

(2) Maritime security issues and initiatives will likely continue to emerge that may appear to be good candidates for potential inclusion in AMSPs.

However, the policy implications associated with emerging significant issues must be resolved before expanding the scope of AMSPs. Therefore, COTPs/FMSCs should seek the concurrence of Commandant (CG-5P), Office of Port and Facility Compliance (CG-FAC), via the cognizant Coast Guard District and Area Commands before expanding the scope of AMSPs to address new issue(s). In a number of instances the issues or level of detail involved may be more appropriately addressed through additional guidance such as field-generated best practices guides, job aids, incident action plan templates, or incident-specific templates to tailor guidance to very specific needs. Such materials may be incorporated by reference in AMSPs where appropriate. Examples of initiatives that are suitable for preparedness planning using AMS planning processes and incorporation by reference are port-level Underwater Terrorism Preparedness Plans (UTPP), Interagency Underwater Preparedness Assessment (IUPA), and Radiation/Nuclear Detection (RAD/NUC) Detection Concept of Operations (CONOP) and Standard Operating Procedures (SOP).

(3) All appendices and annexes included in an AMS Plan are part of the AMSP for which the COTP/FMSC is responsible. Therefore, all information contained in appendices and annexes must go through the formal review and approval process by the plan review and approving authority.

d. The standardized template will also ensure that certain sections of the AMSP, for example MARSEC Level 2 strategies, can easily be located in all AMSPs. The AMSP is considered to be a fundamental part of the Maritime Domain Awareness Program's Maritime Common Operating Picture (MCOP).

e. The AMSP is a comprehensive plan that provides awareness, preparedness, prevention, security response, and system stabilization recovery procedures and coordination, and acts as a communications tool among port stakeholders. Where overlaps occur with other contingency plans, linkages and references should be made within the AMSP.

f. The AMSP is a supporting plan to the National Response Framework (NRF). COTPs/FMSCs are required by COMDTINST 16000.28 (series) to ensure that the AMSP aligns with the NRF. The NRF is designed to ensure that the federal government works effectively and efficiently with state, tribal, territorial, and local agencies to prevent, prepare for, respond to, and recover from domestic incidents using the National Incident Management System (NIMS) protocols.

g. The AMSP is supported by the DHS Maritime Operations Coordination (MOC) Plan as part of the Department's response to threats against the U.S. The MOC Plan acknowledges the unique nature of the maritime domain and

the need for a layered approach to security. The MOC Plan also provides the framework to coordinate operations between the USCG, CBP, ICE, and other international, federal and local agencies.

h. 33 C.F.R. Part 103 requires an AMSC to identify mitigation strategies and implementation methods for use to ensure continued marine operations at an acceptable risk level. For planning purposes, the COTPs/FMSCs and the AMSCs shall identify and list in priority a minimum of three Transportation Security Incident (TSI) scenarios within the COTP Zone, and develop security response procedures for these scenarios. The following guidelines should be used to develop TSI scenarios in order to support the development and exercise of maritime response capabilities. For large port complexes and waterway systems, additional scenarios may be needed to sufficiently address security concerns.

(1) The purpose of identifying three TSI scenarios is to ensure that generic strategies to mitigate risk are developed for the most likely high-risk/consequence maritime threat scenarios in the port, at all MARSEC levels. These scenarios should assist the AMSC in planning, training, and overall preparedness efforts directed towards determining mission essential tasks.

(2) The selection of TSI scenarios should be guided by the output of the AMS Assessment and MSRAM results for the COTP Zone. Critical Infrastructure and Key Resources (CIKR) and maritime systems can be grouped into broad categories (e.g., bridges and tunnels, high capacity passenger vessels, waterfront facilities, Oil/HAZMAT, etc.). These groupings may be adapted from the MSRAM results, prior assessments, and other relevant reports. The highest risk target classes, events, or transits for each broad category of CIKR in MSRAM should be selected as the basis for TSI scenario development within the AMSP.

i. The level of security response planning within the AMSP should be general in nature, and clearly address, at a minimum, the following three elements: (1) what agencies/persons have jurisdiction over the response; (2) the command and control (C2) organization to be used in the response, including the roles and responsibilities for each C2 element, and; (3) what security resources will be used for response to the incident.

j. For planning purposes, unless an increase in threat levels results in a pre-incident shift to Unified Command processes, COTPs/FMSCs and AMSCs should assume that when an incident occurs, first responders and emergency service providers will initially react and function in accordance with their respective authorities. They should also assume for planning purposes that incident management will be shifted to Unified Command as appropriate.

k. Protected Critical Infrastructure Information (PCII). PCII, as defined in 6 U.S.C. 131 (as amended), may be important or essential to planning the recovery of maritime CIKR. Access to PCII will be limited to the purpose for which it was obtained and voluntarily provided by owners of such material. PCII information shall be maintained and safeguarded separately. PCII information will not be included in the AMSP and will be maintained separately. Access to, use of, and safeguarding PCII information will be done in strict accordance with the requirements of 6 C.F.R. Part 29.

l. As the Lead Federal Agency (LFA) for maritime security and the designated Sector Specific Agency (SSA) for the Marine Transportation System, the Coast Guard is responsible for maintaining, safeguarding, and disseminating critical maritime security data. Accordingly, all efforts to compile security plan data in an electronic format should be made. The Coast Guard's HOMEPORT portal will serve as a primary medium for sharing security plan data with port stakeholders when applicable. In addition, secure portals within the Homeland Security Information Network (HSIN) should be used to share security-related information with law enforcement agencies.

m. Recommended Practices:

(1) Security Information: Should access to proprietary information become necessary for MTS recovery planning, such information should be handled outside of the AMSP with provisions for appropriate levels of information protection.

(2) Terminology: As a general rule, language contained in the AMSP should not contain agency specific acronyms or jargon. Plain language shall be used whenever possible. Use standard maritime terminology when referring to specific types of practices, equipment and people.

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

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

(4) Locations: Always include the Map/Digital Nautical Chart (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). Use only geo-coordinates in Latitude and Longitude.

(5) Data Format and Medium: Use 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.

(6) Photography: If photographs are used with the Plan, use digital photography or digitize (scan) standard film photographs. Identify the date the photograph was taken either in the photograph itself or in a caption underneath. Save them as JPEG files to use less digital space.

(7) Imagery: If imagery is used in the AMSP, 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. Identify the date the imagery was taken either in the imagery itself or in a caption underneath the image.

GUIDANCE FOR DEVELOPMENT AND MAINTENANCE OF THE AREA MARITIME SECURITY PLAN (AMSP) TABLE OF CONTENTS

AREA MARITIME SECURITY PLAN TEMPLATE

[TEMPLATE COMPLETION INSTRUCTIONS ARE SHOWN IN ITALICIZED SMALL CAPS. "CUT AND PASTE" TEXT IS SHOWN IN regular *FONT. SUGGESTED TEXT IS SHOWN IN ITALICS. TABLES, WHEN USED TO CONSOLIDATE INFORMATION, SHOULD BE REFERENCED IN THE APPROPRIATE SUBSECTION. EACH PARAGRAPH MUST BE MARKED WITH THE APPROPRIATE CLASSIFICATION LEVEL (E.G., (U), (SSI)). FOR THOSE PARAGRAPHS WHERE THE CLASSIFICATION LEVEL IS DETERMINED AT THE LOCAL LEVEL, EMPTY PARENTHESES HAVE BEEN PLACED INTO THE TEMPLATE AS PLACEHOLDERS TO FACILITATE THIS PROCESS.]*

1000 (U) AREA MARITIME SECURITY PLAN.

1100 (U) Purpose.

(a) (U) The purpose of this Plan is to ensure effective government and private sector security measures are being coordinated in a manner that allows all responding entities to implement plans and procedures designed to deter, detect, disrupt, respond to, and recover from a Transportation Security Incident (TSI) or the threat thereof.

(b) (U) The Captain of the Port (COTP), in consultation with the Area Maritime Security (AMS) Committee for *[INSERT THE NAME OF THE LOCAL COTP ZONE]*, has developed this AMS Plan (AMSP). This plan, when implemented in conjunction with DHS Transportation Systems Sector-Specific Plans (TSS-SP), is designed to deter and recover from a TSI in or near the COTP Zone. A TSI is defined in the Maritime Transportation Security Act of 2002 (MTSA) as "a security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area." A TSI is also included as a type of transportation disruption as defined by the Security and Accountability for Every Port Act of 2006 (SAFE Port Act). This plan also describes the area and infrastructure covered by the plan, including areas of population or special economic, environmental, national security importance that might be damaged by a TSI, and security responses for TSIs. This AMSP provides a primary means for coordination of TSI prevention, protection, security response, and Marine Transportation System (MTS) stabilization and recovery by federal, state, tribal, territorial, and local government organizations, and other port stakeholders.

(c) (U) The AMSP's primary objective is to provide a framework for communication and coordination among port stakeholders and law enforcement officials, and to identify and reduce vulnerabilities and security threats both in and adjacent to the MTS. This AMSP was designed to encourage collaboration among port stakeholders and seeks to capture information necessary to coordinate and

communicate security procedures at each MARSEC Level. This plan complements and encompasses facility and vessel security plans within the *[List USCG COTP Area/Zone for this plan]*. Pursuant to this AMSP, MTS stakeholders will take certain actions contingent upon changes in MARSEC Levels and develop unified preparedness strategies to deter, respond to, and recover from TSIs and other security incidents. The increased security posture includes actions to be taken resulting from a credible threat of a TSI, which necessitates increased prevention and protection measures, or other precautionary security response activities.

(d) (U) Terrorist threats or incidents that result in a breach of security within a respective security plan, process or perimeter, will not always result in a TSI. This AMSP is focused on identifying and implementing measures designed to prevent the occurrence of a TSI. Threats and breaches of security need to be evaluated on a case-by-case basis and responded to accordingly. It is the COTP/FMSC's responsibility to determine if and when an incident occurring in *[LIST USCG COTP ZONE FOR THIS PLAN]* is severe enough to meet the criteria of a TSI. It is also the COTP/FMSC's responsibility to determine if and when the credible threat of a TSI is severe enough to warrant enhanced security measures to deter or respond to a terrorist attack, and the associated recovery measures that will be needed to restore port operations and cargo flow.

1200 (U) Captain of the Port (COTP) Letter of Promulgation.

[INSERT LETTER OF PROMULGATION HERE OR ATTACH TO THE AMSP. A STANDARD TEMPLATE FOR THE LETTER OF PROMULGATION IS PROVIDED AS TAB D TO ENCLOSURE 2]

1210 (U) Record of Changes and Annual Validation

[USE FORM PROVIDED AS TAB C: TO ENCLOSURE 2]

1300 (U) Authority.

(a) (U) The Maritime Transportation Security Act of 2002 (MTSA) (Public Law 107-295, codified at 46 U.S.C. § 70101 – § 70117), mandates the development of DHS Transportation Systems Sector-Specific Plans (TSS-SP), Area Maritime Security Plans, and Facility and Vessel Security Plans. The Security and Accountability for Every Port Act of 2006 (SAFE Port Act) (Public Law 109-347; 46 U.S.C.A. § 70101 et. seq.), established a requirement for inclusion of a Salvage Response Plan in each AMSP. The Coast Guard

Authorization Act of 2010 established the requirement for inclusion of area response and recovery protocols to prepare for, response to, mitigate against, and recover from a TSI. The FAA Reauthorization Act of 2018 authorizes the requirement to incorporate cyber risks into the AMSP to include a process to facilitate sharing of cyber information related to risks and timely reporting. 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 (FMSCs) pursuant to 33 C.F.R. Part 103, are responsible for developing AMSPs in consultation with AMSCs.

(b) (U) The contents of this AMSP, in addition to those mandated by MTSA and the SAFE Port Act, include other security matters consistent with authority provided under the Magnuson Act and Executive Order 10173 (as amended), and the antiterrorism and other security provisions of the Ports and Waterways Safety Act (PWSA) of 1972, for which maritime community engagement is essential.

1310 (U) Federal Maritime Security Coordinator (FMSC)

(a) (U) The COTP, as the FMSC for *[LIST USCG COTP ZONE FOR THIS PLAN]* has the responsibility of establishing the AMSC and developing and maintaining this AMSP and its related AMS Assessment, in close coordination with the AMSC. These responsibilities for security are in addition to key responsibilities for traditional Coast Guard missions and are fundamental to the success of the Maritime Homeland Security (MHS) mission. To accomplish the goals outlined in the Coast Guard's Strategy for Maritime Safety, Security, and Stewardship, the FMSC must rely on fellow federal, state, tribal, territorial and local representatives, and other maritime area partners to assist whenever and however possible.

1400 (U) Scope.

(a) (U) This AMSP is broad in scope, encompassing the maritime domain within the *[LIST USCG AND COTP ZONE FOR THIS PLAN]*, and considers the individual assessments and planning efforts of facilities and vessels operating within the Zone. The scope of this AMSP has been determined by evaluating the waterways, facilities, vessels, and adjacent areas that experience or may be affected by a TSI.

(b) (U) The security plans required by 33 C.F.R. Parts 104-106 provide the foundation of this AMSP. However, this AMSP extends beyond the required facility and vessel security plans and contains strategies

to reduce the vulnerabilities of the port, including those vessels, facilities and infrastructure that are not regulated under 33 C.F.R. Parts 104-106.

1500 (U) Assumptions.

(a) (U) The following suppositions provide the foundation for the Coast Guard's approach to its MHS mission and successful implementation of the MTSA:

(1) (U) Ports are easily accessible by the public (and terrorists), and therefore are susceptible to a TSI, which may occur at any time with little or no warning.

(2) (U) Protection of human life and health are the most important considerations in AMSP development and execution.

(3) (U) Maintaining continuity of operations and facilitating commerce in the port area are key goals for any plan or operation.

(4) (U) Area maritime security must be maintained during the response and recovery phases of TSIs, and during other transportation disruptions.

(5) (U) It is in the best interest of the United States to increase port security through a systems approach, employing robust collaboration and communications between law enforcement agencies, the intelligence community, and port stakeholders.

(6) (U) Each entity directly or indirectly involved with the MTS will participate with the AMSC to increase awareness and prevent illegal acts.

(7) (U) The National Oil and Hazardous Substances Pollution Contingency Plan, National Response Framework, Maritime Operations Coordination Plan, and other response plans may be activated for the purpose of response management following a TSI.

(8) (U) All port areas are vulnerable to an airborne attack. However, planning for mitigation of risk associated with airborne attacks will be limited to information sharing and response (e.g., procedures for communicating threat information among appropriate agencies and stakeholders, planning for evacuation

of facilities/ships threatened by air attack, and post-attack recovery activities).

(9) (U) There will be competition for security, response, and recovery resources as incidents and threat levels increase in number or magnitude.

1600 (U) Situation.

[THIS section ADDRESSES THE REQUIREMENT IN 46 U.S.C. § 70103(b)(2)(B) TO DESCRIBE THE AREA AND INFRASTRUCTURE COVERED BY THE PLAN, INCLUDING THE AREAS OF POPULATION OR OTHER AREAS OF SPECIAL ECONOMIC, ENVIRONMENTAL, OR NATIONAL SECURITY IMPORTANCE THAT MIGHT BE DAMAGED BY A TSI.]

(a) (U) The complexity, scope, and potential consequences of a terrorist threat or TSI occurring within the MTS require that there be a coordinated effort between all MTS users and law enforcement agencies. This effort requires communication and awareness of potential threats and coordinated procedures for preparedness, prevention, protection, response and recovery. It requires 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 AMSP.

1610 (U) Physical Characteristics.

[THE MTS RECOVERY PLAN MAY ALREADY PROVIDE SOME OF THE FOLLOWING REQUIREMENTS, PARTICULARLY PARTS OF (A) (1) (2) (3) (4), AND (5) AND (B). PHYSICAL CHARACTERISTICS NEED TO BE LISTED IN THE AMSP, ENSURE THE DESCRIPTIONS ARE THE SAME IN BOTH PLANS.]

(a) ( ) *[DESCRIBE THE BOUNDARIES OF THE COTP ZONE, OR AREA, THAT THE AMS PLAN COVERS. INCLUDE THE FOLLOWING ITEMS.]*

(1) ( ) *[DESCRIPTION OF IDENTIFIABLE BODIES OF WATER AND RIVERS, SURROUNDING WATERFRONTS AND SIGNIFICANT NAVIGABLE WATERWAYS IN THE PORT AREAS. COVER ALL PORTS INCLUDING RIVER PORTS AND OTHER PORTS IDENTIFIED BY THE PLAN APPROVING AUTHORITY];*

(2) ( ) *[DESCRIPTION OF THE MTS INFRASTRUCTURE, BOTH PHYSICAL FEATURES (E.G., PIERS, DOCKS, AND WHARVES)*

AND INFORMATION SYSTEMS WHICH MAY INCLUDE TELECOMMUNICATIONS, COMPUTER, AND NETWORK SYSTEMS THAT COULD IMPACT INTERNAL INFORMATION TECHNOLOGY AND/OR OPERATIONAL TECHNOLOGY SYSTEMS THAT MAY BE LINKED {E.G., LOCKS, DRAWBRIDGES, EMERGENCY BROADCAST SYSTEMS, ETC.} TO THE MTS];

(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 PORT OPERATIONS CRITICAL TO SIGNIFICANT LOCAL AREA NON-MARITIME FUNCTIONS, SERVICES OR ACTIVITIES (E.G., VESSEL DELIVERY OF FEED STOCKS FOR INDUSTRIAL PRODUCTION; FERRY OPERATIONS THAT TRANSPORT MAJOR SEGMENTS OF THE LOCAL WORK FORCE)];*

(6) ( ) *[DESCRIPTION OF NON-MARITIME CRITICAL INFRASTRUCTURE KEY RESOURCES (CIKR) WITHIN THE COTP ZONE FOR WHICH WATERSIDE SECURITY IS AN ISSUE]*;

(7) ( ) *[DESCRIPTION OF AREAS OF POPULATION OR SPECIAL ECONOMIC, ENVIRONMENTAL, OR NATIONAL SECURITY IMPORTANCE THAT MIGHT BE DAMAGED BY A TSI]*.

(b) ( ) *[DESCRIPTIONS MAY BE GRAPHICALLY DEPICTED ON CHARTS AND MAPS AND INCLUDED IN THE PLAN AS APPENDICES. REFER TO THESE MATERIALS HERE.]*

1620 (U) Economic and Supply Chain Characteristics.

[DO NOT INCLUDE PROPRIETARY INFORMATION OR ANY INFORMATION THAT IS DESIGNATED BY THE TRANSPORTATION SECURITY ADMINISTRATION AS PROTECTED CRITICAL INFRASTRUCTURE INFORMATION (PCII) UNDER 6 C.F.R. PART 29 IN THE AMSP.]

(a) ( ) *[BRIEFLY DESCRIBE MAJOR ECONOMIC ELEMENTS OF THE 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 intermodal connectors.

(3) ( ) Major cargos and major cargo streams including those that involve regional or national economic implications if disrupted (i.e., dependent and interdependent effects).

(4) ( ) Global supply chain connections.

(5) ( ) Recent economic data.

(b) ( ) *[PROVIDE OVERVIEW OF MTS-RELATED INTERDEPENDENCIES. CIKR-SPECIFIC INFORMATION SHOULD BE ASSEMBLED OUTSIDE OF THE AMSP]*.

1630 (U) Charts and Maps.

[INCLUDE CHARTS AND MAPS. THESE MATERIALS SHOULD BE INCLUDED IN APPENDICES.]

1640 (U) Security Zones.

[ADD PRE-ESTABLISHED SECURITY ZONES, INCLUDE CHART-LETS AND/OR OVER-HEAD IMAGES.]

2000 (U) AREA MARITIME SECURITY COMMITTEE.

2100 (U) Introduction.

(a) (U) The Commandant has determined that the AMSC is an essential tool for the development and execution of the AMSP, and for achieving an enhanced level of security within the maritime domain.

(b) (U) The COTP/FMSC has established and convened the AMSC to advise the Coast Guard on maritime security matters pursuant to 33 C.F.R. § 103.300.

2200 (U) Purpose and Objectives.

(a) (U) The AMS Committee brings together experienced representatives from a variety of sources within the *[INSERT THE NAME OF THE LOCAL COTP ZONE]* to continually assess security risks to the ports, determine appropriate risk mitigation strategies, and assist with development, revision, exercise, and implementation of the AMSP.

(b) (U) Under the direction of the COTP, AMSCs are responsible for:

(1) (U) Identifying critical port infrastructure and operations;

(2) (U) Identifying physical and cyber risks (threats, vulnerabilities, and consequences);

(3) (U) Determining mitigation strategies and implementation methods;

(4) (U) 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;

(5) (U) Providing advice to and assisting the COTP in developing the AMSP;

(6) (U) Serving as a link for communicating threats and changes in MARSEC Levels, and disseminating appropriate security information to port stakeholders;

(7) (U) Ensuring that a risk based AMS Assessment and Report are completed and that they meet the requirements specified in 33 C.F.R. § 101.510, § 103.310, § 103.400, and § 103.405.

2300 (U) Charter.

[INSERT A COPY OF THE AMSC'S OFFICIAL CHARTER AS AN APPENDIX AND INCORPORATE BY REFERENCE HERE.]

(U) This AMSC was established on *[INSERT DATE CHARTER WAS PROMULGATED]* under the terms of a written charter in accordance with 33 C.F.R. § 103.300(b). AMSC members should be familiar with Encl (1) of NVIC 9-02 (series).

2310 (U) Committee Structure and Procedural Rules.

[THIS SECTION DESCRIBES AMSC STRUCTURES AND PROCEDURES. STANDING PROCEDURES, SUCH AS REQUIREMENTS FOR A QUORUM, RAISING MOTIONS, RECORD KEEPING, VOTING, TERMS OF OFFICE, DUTIES AND RESPONSIBILITIES AND PARLIAMENTARY PROCEDURES SHOULD BE DOCUMENTED IN THIS SECTION. INCLUDE A LINE DIAGRAM OF THE AMSCS ORGANIZATIONAL STRUCTURE.]

(a) (U) This AMSC will elect one of its appointed members as the Chairperson and one of its appointed 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) (U) The COTP/FMSC will designate a staff member to be the Executive Secretary of the AMSC. 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 electronic and hard copy editions of both the AMSP and AMS Assessment Report. The Executive Secretary is also responsible for ensuring that all committee records are properly maintained and designated as SSI as appropriate, and is responsible for participation in the state, local and industry clearance process. The Executive Secretary is also responsible for ensuring that any information made available for AMSC use, and information designated as Protected Critical Infrastructure Information (PCII) is properly maintained and safeguarded.

(c) (U) Standing Committees will be designated in the charter [e.g., cyber subcommittees, exercise subcommittees, etc.]. Ad hoc sub-committees may be developed on an as-needed basis.

(d) (U) The AMSC will meet whenever requested by the COTP/FMSC, when requested by a majority of the AMSC, or at least once in a calendar year *[QUARTERLY MEETINGS ARE AN AMS PROGRAM GOAL]*. Records of these meetings may be made available to the public upon request. However, COTPs/FMSCs will ensure that all material designated as SSI, PCII or Chemical-Terrorism Vulnerability Information (CVI) is protected from disclosure to the public.

(e) (U) Appointed AMSC members and other participants who have been determined by the COTP/FMSC to be "Covered Persons" with a "need to know" will be provided access to AMSC records that contain SSI material. Access and handling of SSI materials will conform to 49 C.F.R. Part 1520 and be guided by the provisions of NVIC 10-04 and Enclosure (3) to NVIC 03-07, which requires name-based background checks for AMSC appointed members. CG Exec Sec will submit names to CG-FAC for adjudication.

(f) (U) The COTP/FMSC may nominate state, tribal, territorial, local, and industry-appointed members of the AMSC for a security clearance to be sponsored by Coast Guard Headquarters, Office of Port and Facility Compliance, Domestic Ports Division (CG-FAC-1). The COTP/FMSC is responsible for determining the "need to know," assembling and forwarding personnel security investigation packages, and all required training. Procedures for requesting security clearances for AMSC members can be found in Chapter 6 of COMDTINST 5520.12 (series).

2320 (U) Relationship to Other Committees.

(a) (U) The AMSC may be related to other committees. [Include a brief description of listed committee activities/charters and their relationship to the AMSC]

(1) (U) Port Readiness Committee (PRC).

(2) (U) Harbor Safety Committee (HSC).

(3) (U) MTS Committees.

(4) (U) Area Committees (AC).

(5) (U) Other committees as appropriate.

3000 (U) AWARENESS.

3100 (U) Introduction.

[INCLUDE AN EXPLANATION OF MARITIME SITUATIONAL AWARENESS. EXPAND AS APPROPRIATE FOR LOCAL SITUATION.]

(a) (U) This AMSP is intended to be one of the fundamental elements in building situational and maritime domain awareness. This AMSP affords critical decision makers within the *[INSERT THE NAME OF THE LOCAL COTP ZONE]* rapid access to vital information during routine and crisis maritime situations.

(b) (U) Situational awareness developed through this AMSP is complemented by suspicious activity reporting by those owners or operators required to have a VSP or FSP, or by any other person or entity [reporting outlined in citizen-based vigilance] through National citizen watch programs such as the DHS "See Something, Say Something" campaign, coupled with similar regional or local maritime domain awareness initiatives. *[DESCRIBE STATE AND LOCAL PROGRAMS]*.

3200 (U) Federal, State, Tribal, Territorial, Local Security & Law Enforcement Agency Jurisdiction.

[THE AMSP WILL SHOW THE JURISDICTIONAL BOUNDARIES AND AUTHORITIES OF FEDERAL, STATE, TRIBAL, TERRITORIAL, AND LOCAL SECURITY AND LAW ENFORCEMENT AGENCIES WITHIN THE COTP ZONE. USE OF A TABLE FORMAT IS RECOMMENDED FOR MAPS/CHARTS AND COORDINATE LOCATIONS. THESE MATERIALS MAY BE INCLUDED AS AN APPENDIX TO FACILITATE ACCESSIBILITY DURING INCIDENT MANAGEMENT.]

(a) (U) Federal, state, tribal, territorial, and local security and law enforcement jurisdictional boundaries and areas of responsibility. *[WHEN DEPICTING FEDERAL, STATE, TRIBAL, TERRITORIAL, AND LOCAL JURISDICTIONAL BOUNDARIES AND AREAS OF RESPONSIBILITY, FIRST, SECOND AND THIRD TIER RESPONSE AGENCIES WILL BE ADDRESSED SEPARATELY IN THE AMSP. A DESCRIPTION OF EACH AGENCY'S INDIVIDUAL LOCATION AND CAPABILITY WILL GREATLY ENHANCE THE AMSC'S ABILITY TO DETERMINE THE TYPE AND QUANTITY OF RESOURCES THAT MAY RESPOND TO A TSI.]*

(b) (U) Agencies are tiered as follows:

(1) (U) First tier agencies are those such as police, fire, and emergency medical units who are normally dispatched thru the emergency 911 call system.

(2) (U) Second tier agencies are those with special recovery and containment capabilities for dealing with hazardous materials, rough terrain, underwater search and recovery, excavation, or heavy equipment (e.g., mobile heavy-lift cranes).

(3) (U) Third tier agencies are the National Guard, military reserve, and other national level response elements.

(c) (U) Individual agency jurisdictional boundaries may be portrayed on maps or charts in an overlay fashion. The jurisdictional boundary maps may extend outside the AMSC's COTP Zone to reveal neighboring agencies or elements that may be involved in both routine and crisis situations.

3300 (U) Area Maritime Security (AMS) Assessment.

[IDENTIFY THE ASSESSMENT METHODOLOGY INFORMATION AS: WHO, WHERE, WHEN, HOW OBTAINED AND RESULTS.]

(a) (U) This AMSP is prepared based on the AMS Assessment for, *[INSERT THE NAME OF THE LOCAL COTP]*, which is a risk-based analysis of the port(s). The Coast Guard has developed a process consisting of five steps that are discussed in greater detail in Enclosure (3) of the NVIC 09-02 (series).

(b) (U) The five steps in the assessment process are:

(1) (U) Identify critical MTS operations and infrastructure;

(2) (U) Develop attack scenarios;

(3) (U) Conduct consequence and vulnerability assessments for each scenario;

(4) (U) Categorize and prioritize scenarios; and

(5) (U) Develop mitigation strategies for each MARSEC level.

3310 (U) Area Maritime Security Assessment Report.

[THIS SECTION IMPLEMENTS 33 C.F.R. § 103.400 - § 103.410 REGARDING THE AREA MARITIME SECURITY ASSESSMENT. THE AMS ASSESSMENT REPORT SHOULD BE SUMMARIZED IN THIS SECTION. ATTACH IN ITS ENTIRETY AS APPENDIX 9500 UTILIZING TAB B TO ENCLOSURE (2) AS THE RECOMMENDED REPORT TEMPLATE.]

3400 (U) Communications.

[THIS SECTION DESCRIBES THE COMMUNICATION METHODS AND PROCEDURES REQUIRED BY 33 C.F.R. § 103.505]

(a) (U) *[INSERT A DESCRIPTION OF THE COMMUNICATION PROTOCOLS TO BE USED WHEN THE COTP/FMSC DESIRES CONSULTATION WITH THE AMSC. SPECIFIC PROCEDURES SHOULD BE DESCRIBED FOR COMMUNICATING MARITIME SECURITY INFORMATION, EMERGENCY AND NON-EMERGENCY SITUATIONS. IDENTIFY PRIMARY, SECONDARY AND TERTIARY METHODS OF COMMUNICATION. ENSURE THE COMPILATION OF A CONTACT LIST WITH 24/7 CONTACT INFORMATION FOR ALL APPOINTED AMSC MEMBERS AND OTHER PERTINENT ENTITIES.]*

(b) (U) *[INSERT A DESCRIPTION OF THE COMMUNICATION PROTOCOLS TO BE USED WHEN THE COTP/FMSC AND/OR THE AMSC DESIRES TO COMMUNICATE WITH FIRST RESPONDERS, PUBLIC SAFETY OFFICERS, CRISIS MANAGEMENT ORGANIZATIONS, FACILITIES, COMPANIES, VESSELS, MARITIME STAKEHOLDERS, RECREATIONAL BOATERS, VESSEL PILOTS, VESSEL TRAFFIC MANAGEMENT ORGANIZATIONS, GENERAL PUBLIC, WATERWAY USERS, OR OTHER AUDIENCES. PROCEDURES SHOULD BE DESCRIBED FOR COMMUNICATING MARITIME SECURITY INFORMATION IN EMERGENCY AND NON-EMERGENCY SITUATIONS. IDENTIFY PRIMARY, SECONDARY AND TERTIARY METHODS OF COMMUNICATION. ENSURE THE COMPILATION OF A CONTACT LIST WITH 24/7 CONTACT INFORMATION FOR ALL KEY MARITIME STAKEHOLDERS AND OTHER PERTINENT ENTITIES.]*

(c) (U) *[INSERT A DESCRIPTION OF THE COMMUNICATION PROTOCOLS TO BE USED WHEN PRIMARY, SECONDARY, AND TERTIARY METHODS OF COMMUNICATIONS DESCRIBED ABOVE ARE DISRUPTED OR DEEMED UNAVAILABLE DUE TO A CYBER-RELATED EVENT OR OTHER COMMUNICATION DISTURBANCE (E.G., LOSS OF POWER, SYSTEM FAILURE.), WHEN THE COTP/FMSC AND/OR THE AMSC DESIRES TO COMMUNICATE WITH FACILITIES, COMPANIES, VESSELS, RECREATIONAL BOATERS, GENERAL PUBLIC, WATERWAY USERS, AND OTHER MARITIME STAKEHOLDERS AND AUDIENCES. COMMUNICATIONS PROCEDURES SHOULD DESCRIBE HOW (BOTH EMERGENCY AND NON-EMERGENCY) MARITIME SECURITY INFORMATION WILL BE CONVEYED WHEN THE*

PRIMARY METHODS OF COMMUNICATIONS ARE DISRUPTED, AND HOW THEY WILL BE SUSTAINED UNTIL NORMAL COMMUNICATION PROCEDURES ARE REESTABLISHED {DHS HAS PROVIDED THE NATIONAL INTEROPERABILITY FIELD OPERATIONS GUIDE TO ASSIST WITH EMERGENCY COMMUNICATIONS}.]

3400.1 (U) Use of HOMEPORT for Communications.

(a) (U) *[INSERT PROCEDURES FOR USING THE COAST GUARD'S HOMEPORT PORTAL AS A COMMUNICATION AND COORDINATION TOOL FOR THE MARITIME COMMUNITY.]*

3400.2 (U) Use of the Homeland Security Information Network (HSIN) for Communications.

(b) (U) *[INSERT PROCEDURES FOR USING THE HOMELAND SECURITY INFORMATION NETWORK (HSIN) AS A COMMUNICATION AND COORDINATION TOOL FOR THE MARITIME COMMUNITY.]*

3400.3 (U) Use of the Alert Warning System (AWS) for Communications.

(c) (U) *[INSERT PROCEDURES FOR USING THE Alert Warning System (AWS) AS A COMMUNICATION AND COORDINATION TOOL FOR THE MARITIME COMMUNITY [CONSULT COMDTINST 2080.1 USE AND MANAGEMENT OF THE ALERT WARNING SYSTEM AND COMDTINST 5260.5 SERIES ON PII IN REFERENCE TO MASS NOTIFICATION SYSTEMS.]*

3410 (U) Specialized Vessel Communication Systems.

(a) (U) 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.

(b) (U) Ship Security Alert System (SSAS). SOLAS Regulation XI-2/6 requires certain vessels to be outfitted with a SSAS, which allows the vessel to covertly signal a competent authority that the security of the ship is threatened 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. Notifications to federal, state and local law enforcement agencies may be the primary response

to a ship security alert. See Section 5430 for notification and response procedures to a SSAS alert.

(c) (U) Regional Command Center (RCC) Norfolk, also known as the Coast Guard Atlantic Area (LANTAREA) Command Center, and Regional Command Center (RCC) Alameda, also known as the Coast Guard Pacific Area (PACAREA) Command Center are the points of contact (POC) for action and disposition of all SSAS alerts depending on how the service provider sets up the SSAS unit onboard the vessel. The RCCs are the only Coast Guard units that receives the SSAS alerts. The local COTP will not receive the SSAS activation notice; upon receipt of a SSAS alert both RCCs will coordinate with each other to verify location of the alert and notify the command center whose region the alert is located. That command center will take responsibility to contact the company security officer and follow appropriate procedures as outlined in their SSAS Quick Reaction Card (QRC). The following is the contact information list:

- *RCC NORFOLK (LANTAREA COMMAND CENTER) VOICE: 757-398-6700*
- *LANT COMMAND CENTER FAX: 757-398-6775*
- *EMAIL: SSAS@USCG.MIL*
- *RCC ALAMEDA (PACAREA COMMAND CENTER) VOICE: 510-437-3701*
- *PAC COMMAND CENTER FAX: 510-437-3017*
- *EMAIL: SSAS@USCG.MIL*

3420 (U) Reporting TSIs, Breaches of Security, Security Threats, Cyber Intrusions, and Suspicious Activity.

[THIS SECTION DESCRIBES THE PROCEDURES FOR MAKING AND PROCESSING REPORTS OF A TSI, BREACH OF SECURITY, SECURITY THREATS, CYBER INTRUSIONS AND SUSPICIOUS ACTIVITY AS PART OF THE REQUIREMENTS OF 33 C.F.R. § 103.505 AND CG-5P POLICY LETTER 08-16 . THE COMMUNICATION PROTOCOLS IDENTIFIED IN SECTION 3400 WILL BE USED IN CONJUNCTION WITH SPECIFIC FACILITY SECURITY OFFICER OR VESSEL SECURITY OFFICER PROCEDURES DEFINED IN THIS SECTION. THESE PROCEDURES SHOULD COINCIDE WITH

THOSE PROCEDURES CONTAINED IN FACILITY SECURITY PLANS (FSP) AND VESSEL SECURITY PLANS (VSP).]

(a) (U) Owners and operators of facilities required to have a facility security plan under 33 C.F.R. § 101.305 are required to report, without delay, activities that could result in a TSI to the National Response Center (NRC) by telephone at 800-424-8802. 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 are also required to provide this information to the COTP/FMSC directly, without delay. The reports and information garnered as a result of follow-on investigations will formulate intelligence and threat information that may be used to adjust security conditions throughout the country.

(b) For cyber security incidents that do not involve physical or pollution effects, reporting parties may contact the National Cybersecurity and Communications Integration Center (NCCIC), in lieu of NRC, at 888-282-0870.

(c) (U) America's Waterway Watch (AWW) is a national awareness program that encourages 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.

(d) (U) DHS' program "See Something Say Something" urges anyone witnessing suspicious activity to report the incident to the NRC, and to report any immediate danger to life or property by calling 911. More information can be found on the program's website at https://www.dhs.gov/see-something-say-something/become-partner

3430 (U) MARSEC Directives.

(a) (U) When the Coast Guard determines that additional security measures are necessary to respond to either a threat assessment or a specific threat against the maritime elements of the MTS, the Coast Guard may issue a MARSEC Directive setting forth mandatory measures. Only the Commandant or his/her delegate may issue MARSEC Directives. Prior to issuing a MARSEC Directive, the Commandant or his/her delegate will consult with those federal agencies having an interest in the subject matter of that MARSEC Directive. All

MARSEC Directives issued shall be marked as sensitive security information (SSI) in accordance with 49 C.F.R. Part 1520.

(b) (U) When a MARSEC Directive is issued, the Coast Guard will immediately publish a notice in the *Federal Register*, and affected owners and operators will need to go to the COTP or District Commander to acquire a copy of the MARSEC Directive. COTPs and District Commanders will require owners or operators to prove that they are a person required by 49 C.F.R. § 1520.5(a) to restrict disclosure of and access to sensitive security information, and that under 49 C.F.R. § 1520.5(b), they have a need to know sensitive security information.

(c) (U) Each owner or operator of a vessel or facility to whom a MARSEC Directive applies is required to comply with the relevant instructions contained in the MARSEC Directive issued under this section within the time prescribed by that MARSEC Directive.

(d) (U) Each owner or operator of a vessel or facility required to have a security plan under 33 C.F.R. Parts 104, 105 or 106 that receives a MARSEC Directive must:

(e) (U) Within the time prescribed in the MARSEC Directive, acknowledge receipt of the MARSEC Directive to the COTP; and

(f) (U) Within the time prescribed in the MARSEC Directive, specify the method by which the measures in the MARSEC Directive have been implemented (or will be implemented, if the MARSEC Directive is not yet effective).

(g) (U) In the event that the owner or operator of a vessel or facility required to have a security plan under 33 C.F.R. Parts 104, 105, or 106 is unable to implement the measures in the MARSEC Directive, the owner or operator must submit proposed equivalent security measures and the basis for submitting the equivalent security measures to the COTP or, if a facility regulated under 33 C.F.R. Part 106, to their cognizant District Commander, for approval.

(h) (U) The owner or operator must implement the proposed equivalent security measures within the time prescribed in the

MARSEC Directive. The owner or operator must implement any equivalent security measures approved by the COTP, or, if a facility regulated under 33 C.F.R. Part 106, by the cognizant District Commander.

3430.1 (U) Procedures for Communicating MARSEC Directives.

[INCLUDE DETAILED PROCEDURES ON THE DISSEMINATION OF MARSEC DIRECTIVES, INCLUDING WHO WILL GRANT ACCESS TO MARSEC DIRECTIVES, TO WHOM MARSEC DIRECTIVES WILL BE ISSUED. IDENTIFY A SYSTEM FOR TRACKING WHICH PERSONS HAVE BEEN GIVEN ACCESS TO WHAT MARSEC DIRECTIVES. ENSURE THAT ALL PROCEDURES USED IN PROCESSING/DISTRIBUTING MARSEC DIRECTIVES COMPLY WITH THE REQUIREMENTS OF 33 C.F.R. § 101.405. REFER TO THE COMMUNICATION PROTOCOLS AND PROCEDURES LOCATED IN SECTION 3400.]

3430.2 (U) Procedures for Responding to MARSEC Directives.

[IDENTIFY PROCEDURES FOR RECEIVING AND PROCESSING NOTICES OF RECEIPT AND COMPLIANCE WITH MARSEC DIRECTIVES, AND FOR VERIFYING THAT ALL ENTITIES AFFECTED BY THE MARSEC DIRECTIVES ARE IN COMPLIANCE. PROVIDE GENERAL PROCEDURES FOR PROCESSING REQUESTS FOR EQUIVALENT SECURITY MEASURES OR WAIVERS. ENSURE THAT ALL PROCEDURES USED TO PROCESS NOTICES OF RECEIPT AND COMPLIANCE OF MARSEC DIRECTIVES COMPLY WITH THE REQUIREMENTS OF 33 C.F.R. § 101.405.]

3430.3 (U) Role of the AMSC.

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.310(b). THE AMSP WILL DESCRIBE THE ROLE OF THE AMSC IN COMMUNICATING THE ISSUANCE OF A MARSEC DIRECTIVE TO PORT STAKEHOLDERS.]

(a) (U) 33 C.F.R. § 103.310(b) directs the AMSC to serve as a link for communicating threats and changes in MARSEC Levels, and disseminating appropriate security information to port stakeholders. Accordingly, the COTP may from time to time and to different degrees, require the AMSC to assist in the distribution of MARSEC Directives.

(b) (U) *[IN ANTICIPATION OF PROVIDING ASSISTANCE IN THE DISTRIBUTION OF MARSEC DIRECTIVES, THE AMSC SHOULD DEVELOP PROTOCOLS AND PROCEDURES ADDRESSING HOW IT WILL ENSURE THAT DIRECTIVES ARE DISTRIBUTED/RECEIVED IN A*

TIMELY MANNER, AND THE MEANS BY WHICH IT WILL DOCUMENT COMPLIANCE WITH ALL MARSEC DIRECTIVES.]

3440 (U) MARSEC Levels and the National Terrorism Advisory System (NTAS).

[THE AMSP MUST CLARIFY THE RELATIONSHIP BETWEEN THE MARSEC LEVELS, NTAS THREAT ALERTS, AND WHO SETS THE MARSEC LEVEL]

(a) (U) On December 16, 2015, the Department of Homeland Security (DHS) revised the National Terrorism Advisory System (NTAS). The revision added a new form of advisory – the NTAS "Bulletin" – to the existing NTAS "Alerts". This addition provides information describing broader or more general trends and current developments regarding threats of terrorism. They will share important terrorism-related information with the American public and various partners and stakeholders, including in those situations where additional precautions may be warranted, but where the circumstances do not warrant the issuance of an "elevated" or "imminent" Alert. An NTAS Bulletin will summarize the issue and why it is important for public awareness, outline U.S. Government counterterrorism efforts, and offer recommendations to the public on how it can contribute to the overall counterterrorism effort. NTAS Bulletins and Alerts do not automatically lead to changes in MARSEC Level.

(b) (U) The DHS Secretary will issue NTAS Alerts and Bulletins in coordination with other federal entities as appropriate. NTAS Alerts will provide a concise summary of the potential threat, information about actions being taken to ensure public safety, and recommended steps that individuals, communities, businesses, and governments can take to help prevent, mitigate, or respond to the threat. NTAS Bulletins permit the Secretary to communicate critical terrorism information that, while not necessarily indicative of a specific threat against the United States, can reach homeland security partners or the public quickly, thereby allowing recipients to implement necessary protective measures. NTAS Alerts and Bulletins will generally contain an expiration date (i.e., "sunset provision"). They are not intended to be used as generic open-ended "blanket warnings" of the risk of terrorism. DHS may issue updated NTAS Alerts and Bulletins when information regarding the terrorist threat changes. NTAS Alert and Bulletin updates and cancellations will be distributed the same manner as the original notice.

(c) (U) The Coast Guard uses a three-tiered system of MARSEC Levels pursuant to the Maritime Security regulations in 33 C.F.R. part 101. The international community also uses a three-tiered security levels consistent with the MARSEC Levels used by the Coast Guard. MARSEC levels advise the maritime community and the public of the level of risk to the maritime elements of the national transportation system. Ports located in *[INSERT THE NAME OF THE LOCAL COTP ZONE]* will respond to changes in the MARSEC level by implementing applicable measures specified in this plan. Similarly, as specified in the direction to change the MARSEC level, vessels and facilities required to have security plans under 33 C.F.R. Parts 104-106 shall implement the measures specified in their security plans for the applicable MARSEC level.

(1) (U) MARSEC Level 1 is the level of security for which minimum appropriate protective security measures shall be maintained at all times. Unless otherwise directed, each port, vessel, and facility shall operate at MARSEC Level 1.

(2) (U) MARSEC Level 2 is an elevated level of security for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident (TSI).

(3) (U) MARSEC Level 3 is the highest level of security for which further specific protective security measures shall be maintained for a limited period of time when a TSI is probable, imminent (although it may not be possible to identify the specific target), or has already occurred.

(d) (U) The authority to raise or lower the MARSEC Level resides with the Coast Guard Commandant, normally in consultation with the DHS Secretary. MARSEC level changes are usually promulgated via the Coast Guard chain-of-command through Execute Orders (EXORDs). EXORDs customize the MARSEC response based on the circumstances associated with the threat that is driving the change in security posture. MARSEC Level changes may apply nationwide, to a geographic region, or a port. EXORDS can also be used to direct specific PWCS activities, without directing a change in the MARSEC level. EXORDs implementing MARSEC level changes may focus on Coast Guard-only activities, when appropriate. At other times, MARSEC changes/directed

security activities might focus on certain industry sectors of the MTS (e.g., energy, cruise ships, ferries).

(e) (U) MARSEC level changes will be triggered under limited circumstances, in consultation with the DHS Secretary, and usually informed by NTAS Alerts and Bulletins that include threats to the MTS. However, there will also be instances where an imminent or elevated NTAS Alert or an NTAS Bulletin does not threaten or target the MTS. In these instances, the Commandant will evaluate the risk and the appropriate MARSEC level. The Commandant may choose to limit the increase in MARSEC levels to specific ports or port areas in response to a NTAS Alert or Bulletin, versus a broader application of the change in MARSEC (e.g., increasing the MARSEC level at all ports on a particular coast or nationwide). An example of a limited application of MARSEC change authority would be a MARSEC change at ports where Military Outloads (MOL) occur, or at ports considered strategically important.

(f) (U) The COTP may raise the MARSEC level only in exigent circumstances - which are expected to be extremely rare. Such circumstances would include an incident where immediate action to save lives or to mitigate great property or environmental damage resulting in a TSI is required, and timely notification to the Commandant is not possible. If such a circumstance does arise, the COTP will inform the Commandant, via the Coast Guard chain of command, as soon as possible. The higher MARSEC level will remain in effect until lowered by the Commandant. Only the Commandant has the authority to lower the MARSEC Level.

Enhanced Security Measures. The COTP, without raising the MARSEC level, has the ability to impose enhanced security measures using the guidance found in the Maritime Security and Response Operations (MSRO) Manual, M16600.6 (series) - to individual vessels, facilities, or persons. This flexibility addresses emergency security threats in a port and aligns security processes with risks and other considerations. In concert with these actions, the COTP should consider engaging the Commandant and Chain of Command (CoC) via the Critical Incident Communications (CIC) process for visibility and to discuss possibility for Commandant to raise the MARSEC Level.

3440.1 (U) Procedures to Communicate Changes in MARSEC Levels.

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.310(b) AND § 101.300 PROCEDURES FOR PROVIDING NOTIFICATION OF CHANGES IN MARSEC LEVELS, AND 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 C.F.R. PARTS 104, 105, AND 106 ARE INFORMED OF CHANGES IN MARSEC LEVELS.]

(a) (U) Communication protocols and procedures described in Section 3400, and Section 3400.1 above will be used along with Broadcast Notice to Mariners and any other methods deemed necessary by the COTP/FMSC. MARSEC level changes will be announced and obtained in the most expeditious means possible.

3440.2 (U) Notification of MARSEC Level Attainment.

[THE AMSP MUST PROVIDE DETAILED PROCEDURES FOR CONFIRMING COMPLIANCE WITH CHANGES IN MARSEC LEVEL, AND THE CORRESPONDING PRESCRIBED SECURITY MEASURES. ADDITIONALLY, THE AMSP 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. THIS SECTION ALSO DESCRIBES THE PROCEDURES FOR MAKING AND PROCESSING REPORTS OF MARSEC LEVEL ATTAINMENT/COMPLIANCE AS PART OF THE REQUIREMENTS OF 33 C.F.R. § 103.505(g) AND § 101.305. THE PROTOCOLS IDENTIFIED IN SECTION 3400(a), (b), AND (c) IN THIS DOCUMENT WILL BE USED WITH SPECIFIC FACILITY SECURITY OFFICER AND VESSEL SECURITY OFFICER PROCEDURES DEFINED IN THIS SECTION.]

3500 (U) Sensitive Security Information (SSI).

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.505(m). THIS SECTION GOVERNS THE MAINTENANCE, SAFEGUARDING, AND DISCLOSURE OF AMSP INFORMATION, AND OTHER RECORDS AND INFORMATION, THAT HAVE BEEN DESIGNATED AS SENSITIVE SECURITY INFORMATION (SSI), AS DEFINED BY 49 C.F.R. PART 1520 AND NVIC 10-04. REFERENCES (j), (k), and (l) TO NVIC 9-02 CHANGE 5 ALSO PROVIDE ADDITIONAL GUIDANCE ON THE HANDLING AND SAFEGUARDING OF CLASSIFIED AND SENSITIVE BUT UNCLASSIFIED INFORMATION.]

3600 (U) Security Resources.

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.505(g) AND (t). THE AMSP WILL INCLUDE A SECTION THAT LISTS THE SECURITY RESOURCES THAT ARE NORMALLY AVAILABLE IN THE COTP ZONE (CONSIDER RESOURCES IN NEIGHBORING JURISDICTIONS) FOR INCIDENT RESPONSE, THEIR CAPABILITIES, AND WHAT THEIR ESTIMATED TIMEFRAME IS FOR THE DISPATCH OF RESPONDING UNITS. CORRELATE THIS SECTION WITH SECTION 5520 BELOW (PROCEDURES FOR RESPONDING TO A TSI). RESOURCES INFORMATION MAY BE PLACED IN A CONSOLIDATED APPENDIX.]

4000 (U) PREVENTION.

4100 (U) Introduction.

(a) (U) The COTP/FMSC, in consultation with the AMSC, will plan and pre-designate appropriate preventive and protective measures to:

(1) Be conducted at each MARSEC level;

(2) Be continued and adjusted during incident management to aid in stabilizing the situation and to prevent subsequent incidents; and,

(3) Process vessel and cargo flow redirected to the COTP Zone as a consequence of a TSI or significant security issue at other locations.

4200 (U) Maritime Security (MARSEC) Level Planning.

4210 (U) Procedures to Be Used When a Vessel and a Facility Are At Different MARSEC Levels.

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.505(o). THE AMSP WILL IDENTIFY THE COTP/FMSC PROCEDURES TO ENSURE AN INBOUND OR MOORED VESSEL IS INSTRUCTED TO RAISE ITS MARSEC LEVEL, AND WILL DESCRIBE WHAT NOTIFICATIONS ARE REQUIRED TO BOTH VESSELS AND THE COTPS/FMSCS WHEN A FACILITY RECEIVES INFORMATION THAT A VESSEL IS OPERATING AT A LOWER MARSEC LEVEL THAN THE FACILITY. THE AMSP WILL ALSO DESCRIBE CORRECTIVE ACTIONS THAT MUST BE TAKEN.]

(a) (U) When a vessel is operating at a higher MARSEC or security level than the facility or port of 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 or moored vessel, the vessel must attain the corresponding MARSEC level prior to arrival at the port or mooring at the facility per Commandant or COTP/FMSC direction.

4220 (U) Procedures for Requesting Equivalencies to MARSEC Directives.

[DESCRIBE PROCEDURES FOR REQUESTING EQUIVALENCIES FOR SPECIFIC MEASURES REQUIRED BY THE MARSEC DIRECTIVE. THE COTP/FMSC WILL CONVEY APPROVAL OR DENIAL OF EQUIVALENCY REQUESTS USING THE COMMUNICATION PROTOCOLS AND PROCEDURES OUTLINED IN SECTION 3400 OF THIS AMSP.]

(a) (U) In the event that the owner or operator of a vessel or facility required to have a security plan under 33 C.F.R. Parts 104, 105, or 106 is unable to implement the measures in the MARSEC Directive, the owner or operator must submit proposed security measures to the COTP or, if a facility regulated under 33 C.F.R. Part 106, to their cognizant District Commander, for approval.

(b) (U) The owner or operator must submit the proposed equivalent security measures within the time prescribed in the MARSEC Directive. The owner or operator must implement any equivalent security measures approved by the COTP, or, if a facility regulated under 33 C.F.R. Part 106, by their cognizant District Commander.

4300 (U) MARSEC Level 1.

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.505(a)]

4310 (U) Roles, Resources, Authorities, and Responsibilities

[DESCRIBE HOW, AND BY WHOM, SECURITY PROCEDURES ARE IMPLEMENTED.]

4320 (U) Standard Security Procedures for MARSEC Level 1.

[In this section, the AMSP WILL IDENTIFY THE OPERATIONS PLAN (OPLAN) AND/OR OPERATIONAL ORDERS (OPORD) AND EXECUTE ORDERS (EXORD) THAT CONTAIN MARSEC LEVEL 1 PROCEDURES IN EFFECT FOR THE COTP ZONE.]

4330 (U) Physical Security Measures.

[THE AMSP WILL CONSIDER THE FOLLOWING PHYSICAL SECURITY MEASURES WHERE APPROPRIATE FOR MTSA-REGULATED VESSELS AND

FACILITIES, AND VESSELS AND FACILITIES NOT REGULATED UNDER 33 C.F.R. PARTS 104, 105, OR 106.]

(a) (U) Fixed Security Zones (FSZs) and Regulated Navigation Areas (RNA). *[Discuss the planning process for and establishment of FSZs and RNAs, and specify who and how security measures will be enforced.]*

(b) (U) Security Duties and Responsibilities of Port Personnel. *[Incorporate security elements and responsibilities of all port personnel. This may include routine duties, such as observing and reporting malfunctioning security equipment and suspicious persons, activities, and objects.]*

(c) (U) Restricted Areas. *[Include process for establishing and using restricted areas to control access.]*

(1) (U) Restricted Areas. *[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) (U) Marking. *[Discuss marking and signage of restricted areas.]*

(3) (U) Access Control. *[Specify restricted area access control policies and required credentials for entry. Physical security methods such as barriers and fences should be considered.]*

(4) (U) Monitoring. *[Discuss monitoring of 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) (U) Access Points. *[Identify access points to the port, including waterways, rail lines, roadways, walkways, electronic information systems, and adjacent structures and systems.]*

(6) (U) Control Measures. *[Describe control measures for access points, including identification, verification, and purpose and authority for visits.]*

(d) (U) *[Identify specific procedures for notifying vessels and facilities in the COTP Zone that MARSEC Level 1 has been set. Use the communication protocols and procedures outlined in Section 3400 of this AMSP for notification and compliance reporting.]*

(e) (U) *[Designate specific areas where control measures will be implemented.]*

(f) (U) Deny access to anyone refusing to submit to security verification.

(g) (U) *[Describe procedures for monitoring the port, including during the hours of darkness and other times of poor or restricted visibility.]*

(h) (U) Supervision of the handling of cargo and ship's stores. *[Describe cargo security procedures to prevent tampering, or inventory control procedures at access points.]*

(i) (U) Security Review Support. *[Include process that will be used for offering to review physical security plans and procedures for facilities not regulated under 33 C.F.R. Parts 105 or 106 (e.g., public access areas being used for marine events).]*

4340 (U) Cyber Security Measures

[THE AMSP MAY CONSIDER THE FOLLOWING CYBER SECURITY MEASURES WHERE APPROPRIATE FOR MTSA-REGULATED VESSELS AND FACILITIES, AND VESSELS AND FACILITIES NOT REGULATED UNDER 33 C.F.R. PARTS 104, 105, OR 106. ADDITIONAL DETAILED MEASURES CAN BE INCORPORATED BY REFERENCE (E.G., SECTION 9500[EXAMPLE CYBER SECURITY MEASURES FOR EACH MARSEC LEVEL ARE LISTED ON PAGES G-5 TO G-7 OF THE AMS ASSESSMENT JOB AID]) OR INCLUDED HERE. RECOMMEND TO ENGAGE THE AMSC CYBERSECURITY SUBCOMMITTEE OR OTHER SIMILAR GROUPS {E.G., LOCAL FBI INFRAGARD CHAPTER, ETC.}TO ASSIST WITH THIS SECTION.]

(a) (U) Monitoring. *[DISCUSS MONITORING INFORMATION TECHNOLOGY/COMPUTER SYSTEMS THAT IF COMPROMISED/TAMPERED WITH COULD RESULT IN A TSI.]*

(b) (U) Access Points. *[IDENTIFY POTENTIAL ACCESS POINTS TO THE ELECTRONIC INFORMATION SYSTEMS, AND ADJACENT SYSTEMS.]*

(c) (U) Control Measures. *[DESCRIBE CONTROL MEASURES FOR ACCESS POINTS, TO THE ELECTRONIC INFORMATION SYSTEMS AND ADJACENT SYSTEMS.]*

(d) (U) Communicate potential threats as per section 3400.

(e) (U) Policies/Plans/Protocols. *[UPDATE AS NEEDED DUE TO THE FREQUENT AND RAPID ADVANCEMENTS IN TECHNOLOGY.]*

4400 (U) MARSEC Level 2

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.505(b).]

4410 (U) Standard Security Procedures for MARSEC Level 2

[In this section, the AMSP WILL IDENTIFY THE OPERATIONS PLAN (OPLAN) AND/OR OPERATIONAL ORDERS (OPORD) AND EXECUTE ORDERS (EXORD) THAT CONTAIN MARSEC LEVEL 2 PROCEDURES IN EFFECT FOR THE COTP ZONE.]

4420 (U) Roles, Resources, Authorities, and Responsibilities.

[DESCRIBE HOW, AND BY WHOM, SECURITY PROCEDURES WILL BE IMPLEMENTED.]

(a) (U) Within four hours of receiving reports of MARSEC Level 2 attainment, the COTP/FMSC will conduct spot checks of OPSEC measures employed by vessels and facilities, and vessels and facilities not regulated under 33 C.F.R. Parts 104-106, and immediately advise owners/operators of any concerns.

4430 (U) Physical Security Measures.

(a) (U) The AMSP will consider the following physical security measures where appropriate for MTSA regulated vessels and facilities, and vessels and facilities not regulated by 33 C.F.R. Parts 104-106:

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

(2) (U) Review of security roles and responsibilities;

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

(4) (U) Inclusion of mechanisms to ensure that regulated vessels and facilities:

a. (U) Increase the frequency and detail of monitoring of restricted areas;

b. (U) Limit (or further limit) the number of access points (e.g., implement the use of physical means, such as barriers, fencing and security personnel);

c. (U) Increase control of access points (e.g., assigning additional security personnel);

d. (U) Increase detail and frequency of monitoring, including the inspection of individuals, personal effects, and vehicles;

e. (U) Increase frequency of supervised handling of cargo and ship's stores.

(5) (U) Consideration will be given to requiring additional security measures for facilities with a maritime nexus that are not regulated under 33 C.F.R. Parts 105 or 106, (e.g., bridges, tunnels, mass transit bridges/tunnels, stadiums, aquariums, amusement parks, waterfront parks, marine events, and marinas).

4440 (U) Cyber Security Measures

[THE AMSP MAY CONSIDER THE FOLLOWING ENHANCED CYBER SECURITY MEASURES WHERE APPROPRIATE FOR MTSA-REGULATED VESSELS AND FACILITIES, AND VESSELS AND FACILITIES NOT REGULATED UNDER 33 C.F.R. PARTS 104, 105, OR 106. ADDITIONAL DETAILED MEASURES CAN BE INCORPORATED BY REFERENCE (E.G., SECTION 9500[EXAMPLE CYBER SECURITY MEASURES FOR EACH MARSEC LEVEL ARE LISTED ON PAGES G-5 TO G-7 OF THE AMS ASSESSMENT JOB AID]) OR INCLUDED HERE. RECOMMEND TO ENGAGE THE AMSC CYBERSECURITY SUBCOMMITTEE OR OTHER SIMILAR GROUPS {E.G., LOCAL FBI INFRAGARD CHAPTER, ETC.}TO ASSIST WITH THIS SECTION.]

(a) (U) Continuation and enhancement of cyber security procedures required at MARSEC Levels 1;

(b) (U) MARSEC Level 2 measures:

(1) (U) Communicate threats as per section 3400. *[UTILIZE ALL AVAILABLE METHODS TO COMMUNICATE THREAT INFORMATION TO PORT PARTNERS.]*

(2) (U) Policies/Plans/Protocols. *[FOLLOW GUIDANCE PROVIDED.]*

4500 (U) MARSEC Level 3.

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.505(b) AND (h).]

4510 (U) Standard Security Procedures for MARSEC Level 3.

[In this section, the AMSP WILL IDENTIFY OPERATIONS PLAN (OPLAN) AND/OR OPERATIONAL ORDERS (OPORD) AND EXECUTE ORDERS (EXORD) THAT CONTAIN MARSEC LEVEL 3 PROCEDURES IN EFFECT FOR THE COTP ZONE.]

THE AMSP WILL SPECIFY THE COTP/FMSC REVIEW PROCESS FOR MARSEC LEVEL 3 REQUIREMENTS IN CURRENT COAST GUARD AREA OPLAN AND/OR OPORD AND EXORD.]

4520 (U) Roles, Resources, Authorities, and Responsibilities.

[DESCRIBE HOW, AND BY WHOM, SECURITY PROCEDURES WILL BE IMPLEMENTED.]

(a) (U) Within one hour of receiving reports of MARSEC Level 3 attainment, the COTP/FMSC will begin checks of MARSEC measures employed by MTSA regulated vessels and facilities, and vessels and facilities not regulated under 33 C.F.R. Parts 104, 105 and 106, and immediately advise the owner/operator of any violations.

4530 (U) Physical Security Measures.

[THE AMSP MUST CONSIDER THE FOLLOWING PHYSICAL SECURITY MEASURES WHERE APPROPRIATE FOR MTSA REGULATED VESSELS, FACILITIES, AND VESSELS OR FACILITIES NOT REGULATED IN 33 C.F.R. PARTS 104, 105 OR 106.]

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

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

(1) (U) 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 security patrols;

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

(c) (U) Consideration will be given to requiring additional security measures for facilities not regulated under 33 C.F.R. Parts 105 or 106.

4540 (U) Cyber Security Measures

[THE AMSP MAY CONSIDER THE FOLLOWING ENHANCED CYBER SECURITY MEASURES WHERE APPROPRIATE FOR MTSA-REGULATED VESSELS AND FACILITIES, AND VESSELS AND FACILITIES NOT REGULATED UNDER 33 C.F.R. PARTS 104, 105, OR 106. ADDITIONAL DETAILED MEASURES CAN BE INCORPORATED BY REFERENCE (E.G., SECTION 9500[EXAMPLE CYBER SECURITY MEASURES FOR EACH MARSEC LEVEL ARE LISTED ON PAGES G-5 TO G-7 OF THE AMS ASSESSMENT JOB AID]) OR INCLUDED HERE. RECOMMEND TO ENGAGE THE AMSC CYBERSECURITY SUBCOMMITTEE OR OTHER SIMILAR GROUPS {E.G., LOCAL FBI INFRAGARD CHAPTER, ETC.}TO ASSIST WITH THIS SECTION.]

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

(b) (U) MARSEC Level 3 measures:

(1) (U) Communicate threats as per section 3400. *[UTILIZE ALL AVAILABLE METHODS TO COMMUNICATE THREAT INFORMATION TO PORT PARTNERS.]*

(2) (U) Policies/Plans/Protocols. [*FOLLOW GUIDANCE PROVIDED.]*

4600 (U) Public Access Facility (PAF).

(a) *[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.505(w).]* An owner or operator of a facility may request an exemption from the requirements of 33 C.F.R. Part 105 by requesting a determination from the COTP that their Facility meets the definition of a PAF as provided in 33 C.F.R. § 105.110.

4610 (U) Public Access Facilities (PAF).

[IDENTIFY ALL DESIGNATED PUBLIC ACCESS FACILITIES (PAF) WITHIN THE COTP ZONE INCLUDING THE SECURITY MEASURES THAT MUST BE IMPLEMENTED AT EACH PAF DURING EACH MARSEC LEVEL [AS PER GUIDANCE FROM 33 C.F.R. 103.505(W) AND THE PAF JOB AID]. (THESE SECURITY MEASURES SHOULD BE REFLECTED AS A CONDITION OF THEIR PAF DESIGNATION.) ENSURE THERE IS UPDATED 24/7 CONTACT INFORMATION FOR THE INDIVIDUAL THAT IS RESPONSIBLE FOR IMPLEMENTING THE SECURITY MEASURES. THE AMS ASSESSMENT SHOULD INCLUDE THE RECOMMENDED MITIGATION STRATEGIES].

4700 (U) Maritime Worker Credentials.

[THIS SECTION IS USED TO DESCRIBE MARITIME WORKER CREDENTIALS AND THE ROLE THEY PLAY IN THE CONNECTIVITY OF THE FACILITY AND VESSEL SECURITY PLANS AND THE AMSP THUS ENHANCING THE OVERALL SECURITY POSTURE THROUGHOUT THE COTP ZONE. THERE IS SUGGESTED LANGUAGE PROVIDED IN 33 C.F.R. § 101.514 AND § 101.515 DESCRIBING THE TRANSPORTATION WORKER IDENTIFICATION CARD (TWIC) PROGRAM. DESCRIBE ANY ADDITIONAL LOCAL SECURITY IDENTIFICATION REQUIREMENTS FOR DESIGNATED RESTRICTED AREAS WITHIN THE COTP ZONE.]

[IDENTIFY ALL MARITIME TRANSPORTATION WORKER CREDENTIALS REQUIRED AND ACCEPTABLE FOR PORT ACCESS]

5000 (U) SECURITY RESPONSE.

[RESPONSE IN THE CONTEXT OF THIS SECTION IS PRIMARILY DESIGNED TO GUIDE A COORDINATED SECURITY RESPONSE DURING PERIODS OF HEIGHTENED THREAT, AND FOR POST-INCIDENT CONSEQUENCE MITIGATION. IT IS INTENDED TO MAINTAIN AN APPROPRIATE LEVEL OF MARITIME SECURITY DURING THE INITIAL PHASES (FIRST RESPONSE) OF A TSI OR THREAT OF TSI, AND TO GUIDE THE POST-INCIDENT RECOVERY OF THE MTS.

THIS SECTION MUST INCLUDE, AT A MINIMUM, THE FOLLOWING ELEMENTS:

- *THE AMSC'S ROLE RELATIVE TO SECURITY RESPONSE.*
- *PROCEDURES FOR CHANGING MARSEC LEVELS;*
- *PREVENTIVE MEASURES THAT SHOULD BE CONTINUED DURING RESPONSE (TO STABILIZE THE SITUATION AND PREVENT FURTHER DAMAGE AND DETER SUBSEQUENT INCIDENTS);*
- *PROTECTIVE MEASURES (FOR THE MTS AND MARITIME CIKR);*
- *SECURITY RESPONSES BELOW THE LEVEL OF A TSI;*
- *TSI PLANNING SCENARIOS;*
- *NOTIFICATION AND RESPONSE PROCEDURES FOR A TSI;*
- *DRAFT INCIDENT MANAGEMENT STRUCTURE; AND*
- *MEASURES NEEDED TO SET THE STAGE FOR MTS RECOVERY.]*

5100 (U) Introduction.

(a) (U) Section 5000 of the AMSP has been developed by the *[NAME GEOGRAPHIC AREA]* COTP, in consultation with the *[NAME PORT AREA]* AMSC, and is based on an AMS Assessment completed on *[INSERT DATE]* and meets the provisions of 33 C.F.R. § 103.400.

(b) (U) Due to the range of possibilities of a TSI and or threats of TSI, this section is primarily designed to guide the coordinated security response for post-incident consequence mitigation among the area/port stakeholders, to maintain an appropriate level of maritime security during the initial phases (first response) to an incident, and to

guide coordinated response measures that are needed for post-incident recovery of the MTS.

(c) (U) For the purposes of the AMSP, security response to support resumption of trade consists of those measures, operations, and activities in incident areas that are needed to set the stage for MTS recovery activities as described in Sections 5600 and 6000.

5110 (U) Changing MARSEC Levels.

[THIS SECTION IMPLEMENTS 33 C.F.R. § 103.505(b) FOR MARSEC LEVELS 2 AND 3 AS THE RESULT OF A THREAT OF A TSI OR THE OCCURRENCE OF AN ACTUAL TSI. SPECIFY MEASURES AND PROCEDURES THAT WILL BE USED. AMSC MEMBERS WILL USE THE COMMUNICATION PROTOCOLS AND PROCEDURES DESCRIBED IN SECTION 3400 (b) AND (c) ALONG WITH ANY OTHER MEANS AND PROCEDURES DIRECTED BY THE COTP/FMSC TO COMMUNICATE MARSEC LEVEL CHANGES. CROSS-REFERENCE TO SECTION 3440. INCLUDE ANY ADDITIONAL GUIDANCE FOR THE RESPONSE PHASE.]

(a) (U) The procedures for MARSEC level changes specified in Section 3440 will apply during incident management, inclusive of response and recovery phases.

(b) ( ) *[INSERT THE COTP/FMSC'S LOCAL PROCEDURES FOR MARSEC CHANGES DURING THE RESPONSE PHASE.]*

[IN THE SUBSECTIONS THAT FOLLOW, DESCRIBE AND DISCUSS AMS MEASURES THAT ASSIST IN STABILIZING THE SITUATION, SUCH AS PREVENTING FURTHER DAMAGE OR THREATS, PROTECTING PRE-IDENTIFIED CIKR, ASSESSING DAMAGES TO THE MTS, SETTING THE STAGE FOR MTS RECOVERY, AND SUPPORTING THE RESUMPTION OF TRADE. CROSS-REFERENCE TO SECTION 3000 AND 4000 ELEMENTS WHERE APPROPRIATE.]

5200 (U) Preventive Measures.

(a) (U) Prevention activities specified in Section 4000 of this Plan occur during response and recovery phases of an incident. The additional protective measures and procedures in the following subsections apply.

5210 (U) Dangerous Substances and Devices.

(a) (U) Measures to prevent the introduction of dangerous substances and devices into designated restricted areas within the port.

[THIS SUBSECTION IMPLEMENTS 33 C.F.R. § 103.505(e). SPECIFY MEASURES AND PROCEDURES THAT WILL BE USED.]

5220 (U) Unauthorized Access.

(a) (U) Measures to prevent unauthorized access to designated restricted areas within the port.

[THIS SUBSECTION IMPLEMENTS 33 C.F.R. § 103.505(f). SPECIFY MEASURES AND PROCEDURES THAT WILL BE USED.]

5300 (U) Protective Measures.

[INCLUDE IN THIS SECTION PROCEDURES FOR ACTIVE MEASURES TO PROTECT THE AOR BEYOND PREVENTION MEASURES USED FOR BASIC DETERRENCE DURING MARSEC LEVEL 1.]

5310 (U) Procedures for Vessel Quarantine or Isolation.

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.505(g). INCLUDE IN THIS SECTION, OR INCORPORATE BY REFERENCE, THE PROCEDURES THAT MAY BE USED FOR VESSEL QUARANTINE OR ISOLATION, AND RESPONSES TO ADDRESS PUBLIC HEALTH (E.G., PANDEMIC FLU, EBOLA VIRUS) OR OTHER BIOLOGICAL ISSUES (E.G., AGRICULTURAL BIOLOGICAL THREAT) THAT ALSO RAISE SECURITY CONCERNS. IN GENERAL, THE APPROPRIATE APPROACH IS TO LINK EXISTING VESSEL QUARANTINE AND ISOLATION PLANS AND PROCEDURES TO THE AMSP. IDENTIFY AND PROVIDE LINKS TO APPLICABLE FEDERAL, STATE, LOCAL, TRIBAL AND TERRITORIAL QUARANTINE/ISOLATION PLANS. REFERENCE THE MOU BETWEEN THE DEPARTMENT OF HEALTH AND HUMAN SERVICES AND THE DEPARTMENT OF HOMELAND SECURITY DATED OCTOBER 12, 2005. SEE ALSO COMDTINST 6220.11, COAST GUARD RESPONSE TO QUARANTINE COMMUNICABLE DISEASE OUTBREAKS OF OPERATIONAL SIGNIFICANCE.]

5320 (U) Procedures for Security Segregation of Vessels.

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.505(e), (f) AND (g). INCLUDE IN THIS SECTION THE PROCESSES THAT WILL BE USED TO IDENTIFY LOCATIONS TO SEGREGATE A VESSEL OR VESSELS THAT RAISE

SECURITY CONCERNS {IF THE LOCATIONS IDENTIFIED ARE THE SAME AS THE ONES FOR QUARANTINE/ISOLATED VESSELS, REFERENCE SECTION 5310}. ALSO INCLUDE OR INCORPORATE BY REFERENCE PROCEDURES FOR COORDINATING MANAGEMENT OF THE SITUATION.

PRE-DESIGNATION OF LOCATIONS WITHIN OR ADJACENT TO ANY GIVEN PORT AREA SHOULD REFLECT THE POTENTIAL DEMANDS OF THE CIRCUMSTANCES OR THREATS ASSOCIATED WITH A VESSEL-BORNE MARITIME THREAT. A REMOTE LOCATION, ONE THAT AFFORDS A SAFE DISTANCE FROM POPULATED AREAS AND CIKR, AND OTHER VESSELS SHOULD BE FACTORED INTO THE IDENTIFICATION PROCESS. THE COTP/FMSC AND AMSC SHOULD CONSIDER RISK, OFFLOADING RESOURCES, LIABILITY, CAPABILITIES OF FEDERAL, STATE, AND LOCAL LAW ENFORCEMENT AGENCIES, CONSEQUENCE MITIGATION RESOURCES IN DETERMINING WHICH AGENCY OR AGENCIES WILL RESPOND, AND OTHER RELEVANT ISSUES. SUGGESTED CORE TEXT IS PROVIDED BELOW.]

(a) (U) Identification of Prospective Segregation Locations. [The COTP/FMSC, in consultation with the AMSC, will identify prospective anchorages and mooring facilities within the AOR sufficient for the purpose of segregating a vessel or vessels due to security concerns regarding the vessel's cargo or crew.]

[DEVELOP A LIST OF PROSPECTIVE LOCATIONS WITH SUPPORTING DETAIL. THE LIST MAY BE INCLUDED AS AN APPENDIX, MAINTAINED SEPARATELY WITH AN APPROPRIATE LEVEL OF INFORMATION SECURITY, OR INCORPORATED AS A REFERENCE WHERE AN EQUIVALENT LIST IS AVAILABLE.]

(b) (U) Procedures for Cargo Inspection. *[THE NEED FOR CARGO OPERATIONS, SUCH AS CONTAINER REMOVAL OR OFFLOADING OF BULK CARGO, TO INVESTIGATE SAFETY OR SECURITY CONCERNS, WILL BE ASSESSED AT THE TIME OF THE EVENT TO DETERMINE AN APPROPRIATE APPROACH AND PRECAUTIONS THAT MAY BE APPROPRIATE TO THE SITUATION.]*

5330 (U) Procedures for Port and Vessel Evacuation.

[THIS SECTION IMPLEMENTS 33 C.F.R. § 103.505(i). IDENTIFY IN THIS SECTION PROCEDURES THAT WILL BE USED TO IDENTIFY THE NEED FOR AND, IF NECESSARY, CONDUCT AN EVACUATION. INCLUDE WHICH ENTITIES ARE RESPONSIBLE FOR ASSESSING AND DETERMINING WHEN AN EVACUATION OF THE PORT, A SECTION OF THE PORT, OR PORT AREA (INCLUDING SURROUNDING POPULATED AREAS THAT MIGHT BE THREATENED) IS NEEDED AS A RESPONSE TO SECURITY THREATS OR

BREACHES OF SECURITY. ALSO IDENTIFY ASSOCIATED AUTHORITIES OF FEDERAL, STATE, TRIBAL, TERRITORIAL, AND LOCAL OFFICIALS WHICH ARE RESPONSIBLE FOR ORDERING, COORDINATING AND FACILITATING THE EVACUATION TO INCLUDE MARINAS AND SURROUNDING WATERFRONT AREAS.]

[ALL PORTS COVERED IN THIS AMSP WILL BE ADDRESSED. THEREFORE, THE AMSP MUST ALSO ADDRESS THE SITUATION IN WHICH AN EVACUATION MAY BECOME NECESSARY AS A SECURITY OR EMERGENCY RESPONSE TO SPILLOVER EFFECTS FROM A MARITIME SECURITY INCIDENT OR ACTUAL OR POTENTIAL EFFECTS TO THE MTS FROM A NON-MARITIME SECURITY INCIDENT. ENSURE PORT EVACUATION PROCEDURES ARE ALIGNED WITH STATE, TRIBAL, TERRITORIAL, AND LOCAL EVACUATION PLANS.]

[THE COTPS/FMSCS AND AMSC SHOULD CONSIDER THE AUTHORITIES, CAPABILITIES, AND CAPACITY OF FEDERAL, STATE, TRIBAL, TERRITORIAL, AND LOCAL LAW ENFORCEMENT AND CONSEQUENCE MANAGEMENT ORGANIZATIONS WHEN PLANNING AND CONDUCTING EVACUATION OPERATIONS. THE COTPS/FMSCS, IN CONSULTATION WITH THE AMSC, MAY FACILITATE PREPARATION AND POPULATION OF AN INCIDENT ACTION PLAN TEMPLATE OR JOB AID. SUCH MATERIALS, IF PREPARED, MAY BE INCORPORATED BY REFERENCE IN THIS SUBSECTION, AN APPENDIX, OR INCORPORATED AS AN AMSP ANNEX.]

5400 (U) Security Responses to Threats Below the Level of a TSI.

[THIS SUBSECTION IMPLEMENTS IN PART 33 C.F.R. § 103.505(G). INCLUDE GENERAL PROCEDURES OR APPROACHES FOR ADDRESSING THREATS THAT DO NOT RISE TO THE LEVEL OF A TSI.]

[COTPS/FMSCS MAY, IN CONSULTATION WITH AMSCS, OTHER GOVERNMENT AND NON-GOVERNMENT ORGANIZATIONS, DEVELOP AND POPULATE INCIDENT ACTION PLAN (IAP) TEMPLATES OR CONTINGENCY PLANS FOR UNIFIED, PRE-INCIDENT SECURITY RESPONSES TO THREATS THAT ARE BELOW THE LEVEL OF A TSI. THE COTPS/FMSCS MAY INCORPORATE SUCH MATERIALS BY REFERENCE IN THIS SUBSECTION. APPROVAL AND ACTUAL IMPLEMENTATION OF IAPS OR CONTINGENCY PLANS MAY BE UNDER MEMORANDUM OF AGREEMENT OR OTHER SUITABLE VEHICLE WITH ENTITIES TO WHICH A PRE-INCIDENT IAP APPLIES, OR OBSERVING ICS PRINCIPLES IF IMPLEMENTED UNDER A UNIFIED COMMAND.]

(a) (U) 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 miscommunication, lost credentials, an innocent person unaware of entry restrictions or

perimeters, etc. In most of these cases, resolution of the problem or referral to appropriate authorities is the only action needed. In other cases, a law enforcement or security response may be required. Incidents that reveal serious discrepancies or weaknesses within required plans should be reported to the COTP/FMSC.

(b) *(U)* [*INSERT GENERAL PROCEDURE OR APPROACH FOR ADDRESSING THREATS THAT DO NOT RISE TO THE LEVEL OF A TSI. FOR EXAMPLE, COTPS MAY USE ENHANCED SECURITY MEASURES LISTED IN THE MSRO MANUAL AS PER THE APPLICABLE MARSEC LEVEL AND INCORPORATE THROUGH MOUS/MOAS, OTHER GOVERNMENT AGENCIES (OGA) ACTIONS.]*

5410 (U) Procedures for Responding to Suspicious Activity.

[THIS SECTION IMPLEMENTS IN PART 33 C.F.R. § 103.505(g). INCLUDE IN THIS SECTION THE RESPONSE PROCEDURES THAT WILL BE IMPLEMENTED IN THE EVENT OF A REPORT OF SUSPICIOUS ACTIVITY WITHIN THE COTP/FMSC AOR. {MTSA REGULATED ENTITIES SHOULD BE FOLLOWING THEIR APPROVED SECURITY PLAN PROCEDURES}. INCLUDE EXPECTED TIMEFRAMES FOR RESPONDING TO SECURITY THREATS OR BREACHES OF SECURITY, INCLUDING PROVISIONS FOR MAINTAINING INFRASTRUCTURE AND OPERATIONS IN THE PORT {MAY LINK AS APPROPRIATE TO OTHER APPLICABLE PLANS}. THE CONTENT FOR THIS SUBSECTION MAY BE INCLUDED IN A SEPARATE APPENDIX, FOR EXAMPLE, TO ADDRESS AND PROVIDE INFORMATION SECURITY FOR LAW ENFORCEMENT SENSITIVE INFORMATION.]

(a) (U) Reporting of suspicious activity will be in accordance with the communication protocols and procedures listed in Sections 3400 and 3420 of this plan.

(b) (U) [*Insert procedures for reporting suspicious activity to the COTP/FMSC using communications protocols and procedures contained in Section 3400.*]

5420 (U) Procedures for Responding to Breaches of Security.

[THIS SECTION IMPLEMENTS, IN PART, 33 C.F.R. § 103.505(g). INCLUDE IN THIS SECTION ENTITIES RESPONSIBLE FOR RESPONDING TO BREACHES OF SECURITY. THE AMSC WILL CONSIDER JURISDICTIONAL AND GEOGRAPHIC CAPABILITIES OF FEDERAL, STATE, TRIBAL, TERRITORIAL, AND LOCAL LAW ENFORCEMENT AGENCIES AND CONSEQUENCES MITIGATION RESOURCES IN DETERMINING WHICH AGENCY OR AGENCIES WILL RESPOND TO BREACHES OF SECURITY AT

HIGH CONSEQUENCE TARGETS. THE CONTENT FOR THIS SUBSECTION MAY BE INCLUDED IN A SEPARATE APPENDIX, FOR EXAMPLE, TO ADDRESS AND PROVIDE INFORMATION SECURITY FOR LAW ENFORCEMENT SENSITIVE INFORMATION.]

(a) (U) Pursuant to 33 C.F.R. § 101.105, a "Breach of Security" is defined as "an incident that has not resulted in a transportation security incident, in which security measures have been circumvented, eluded or violated."

(b) (U) *[Insert procedures for responding to breaches of security {both for physical and cyber related incidents}.]*

5430 (U) Procedures for Responding if a Ship Security Alert System (SSAS) has been Activated.

[THIS SUBSECTION IMPLEMENTS 33 C.F.R. § 103.505(p). INSERT PROTOCOLS AND PROCEDURES FOR RESPONDING TO AND PROCESSING SSAS ALERTS OCCURRING WITHIN OR NEAR THE AOR ONCE THE COTP IS NOTIFIED BY THE RCC. REFERENCE SECTION 3410 (U) SPECIALIZED VESSEL COMMUNICATION SYSTEMS. SECURITY ALERT SYSTEM AND THE AREA QRC-SHIP SECURITY ALERT SYSTEM. THE CONTENT FOR THIS SUBSECTION MAY BE INCLUDED IN A SEPARATE APPENDIX, FOR EXAMPLE, TO ADDRESS AND PROVIDE INFORMATION SECURITY FOR LAW ENFORCEMENT SENSITIVE INFORMATION.]

5440 (U) Request for Forces (RFF)/Request for Assistance (RFA) Process.

(a) (U) All RFF/RFAs will be routed through the appropriate CG Chain of Command to Commandant, Office of Counterterrorism and Defense Operations Policy (CG-ODO).

5500 (U) Transportation Security Incident Planning Scenarios.

[THIS SECTION WILL DESCRIBE THE TYPES OF TSIS MOST LIKELY TO OCCUR WITHIN THE COTP ZONE'S AOR, AND WILL INCLUDE THE PROCEDURES AND STEPS THAT WILL BE TAKEN TO RESPOND TO EACH LISTED TSI SCENARIO. BECAUSE EACH PORT AREA HAS UNIQUE CHARACTERISTICS, DIFFERENT TYPES OF TSIS ARE LIKELY TO OCCUR MORE FREQUENTLY IN ONE PORT AREA THAN ANOTHER. COTPS/FMSCS SHOULD USE THE RESULTS OF THE AMS ASSESSMENT AND MSRAM DATA TO IDENTIFY THE THREE TYPES OF TSIS MOST LIKELY TO OCCUR WITHIN THE COTP ZONE. THE COTP/FMSC MAY ADD ADDITIONAL TSI SCENARIOS AS NECESSARY.]

[TSI SCENARIO DEVELOPMENT IS GUIDED BY MSRAM RISK INDEX NUMBER AND LOCAL KNOWLEDGE. SCENARIO DEVELOPMENT SHOULD ALSO CONSIDER THREATS TO THE COMMON INFRASTRUCTURE, GENERAL PORT THREATS, AND THOSE THREATS THAT AFFECT OTHER REGULATED VESSELS OR FACILITIES, AND SEVERAL TYPES OF SCENARIOS TO ENSURE MOST PORT STAKEHOLDERS ARE INVOLVED IN PLANNING EFFORTS. ACCORDINGLY, OPTIONAL SCENARIOS MAY BE DEVELOPED FOR TSIS THAT ARE LESS LIKELY TO OCCUR SO THAT THERE IS 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.]

[FOR AMSP UPDATES, IT IS NOT ENVISIONED THAT THIS SECTION WILL REQUIRE THE LEVEL OF DETAIL NECESSARY IN DRAFTING AN INCIDENT ACTION PLAN (IAP). THE AMSP SHOULD TAKE THE AMS COMMUNITY TO THE POINT AT WHICH IC/UC PROCESS IS ESTABLISHED. AMSPS SHOULD PROVIDE FOR CONTINUED PREVENTION AND SECURITY RESPONSE DURING INCIDENT MANAGEMENT.]

[SINCE IT IS IMPOSSIBLE TO PLAN FOR EVERY SCENARIO, THE COTP/FMSC, IN CONSULTATION WITH THE AMSC, SHALL 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.]

5510 (U) TSI Scenarios.

5511 ( ) TSI Scenario One. *[Insert TSI Scenario]*

5512 ( ) TSI Scenario Two. [*Insert TSI Scenario*]

5513 ( ) TSI Scenario Three. [*Insert TSI Scenario*]

5514 ( ) TSI Scenario Four. [*Discretionary*]

5520 (U) Procedures and Resources for Responding to a TSI.

[THIS SECTION IMPLEMENTS 33 C.F.R. § 103.505(t) AND § 103.505(u). FOR EACH OF THE THREE REQUIRED SCENARIOS, THE AMSP WILL INCLUDE AN INCIDENT COMMAND SYSTEM FLOW CHART AND RESOURCE LIST IDENTIFYING THE ASSIGNED ROLES OF THE PRIMARY RESPONDERS TO THE INCIDENT AND IDENTIFY THE JURISDICTION OF THOSE RESPONDING, WHAT RESOURCES THEY WILL PROVIDE, AND THEIR RESPECTIVE CAPABILITIES. THESE DOCUMENTS CAN BE INCLUDED IN THE SCENARIOS ABOVE. ALIGN PROCEDURES USED WITH SECTION 3400 (COMMUNICATIONS) AND SECTION 3600 (SECURITY RESOURCES) IN THIS

PLAN. USE OF AN APPENDIX IS SUGGESTED TO FACILITATE MODIFICATIONS WHEN THERE ARE SIGNIFICANT CHANGES IN PROSPECTIVE INCIDENT RESPONSE RESOURCES.]

5530 (U) Linkage with Applicable Federal, State, Local, Tribal, Territorial and Port Plans.

[FOR EACH OF THE THREE REQUIRED TSI TYPES, IDENTIFY WHAT OTHER RELEVANT FEDERAL, STATE, TRIBAL, TERRITORIAL, AND LOCAL PLANS (E.G., CONCEPT OF OPERATION PLANS FOCUSED ON ACTIVE THREATS SUCH AS ACTIVE SHOOTER AT MASS GATHERINGS) MAY BE IMPLEMENTED AS A RESULT OF THE SCENARIO. MAY BE PREPARED AS A TABLE IN LIEU OF SEPARATE PARAGRAPHS.]

5531 (U) Underwater Terrorism Preparedness Plans (UTPPs).

*[THE COTP/FMSC, IN CONSULTATION AND COORDINATION WITH THE AMSC AS APPROPRIATE, WILL ENSURE THAT APPROPRIATE PREPAREDNESS MEASURES EXIST TO ADDRESS UNDERWATER TERRORISM THREAT PREVENTION, DETECTION, AND RESPONSE IF THEY HAVE IDENTIFIED AN UNDERWATER THREAT VECTOR IN ONE OF THEIR TOP THREE TSIS SCENARIOS. AN UTPP OR AN INTERAGENCY UNDERWATER PORT ASSESSMENT (IUPA) [*SEE BELOW] SHALL BE INCORPORATED BY REFERENCE AS A STANDALONE PLAN IN THIS SECTION OR MAY BE INCLUDED AS AN ANNEX TO THE AMSP. AMSCS THAT HAVE NOT IDENTIFIED AN UNDERWATER THREAT AS A TOP TSI, BUT MAINTAIN A UTTP OR IUPA, HAVE THE OPTION TO REFERENCE THE PLAN].*

*[*THE PESIEDON MEMORANDUM OF AGREEMENT (MOA) BETWEEN USNORTHCOM AND PAC/LANT AREAS PROVIDES THE PROCESS AND TASKS TO IDENTIFY PORTS EACH YEAR FOR DEVELOPMENT OF AN INTERAGENCY UNDERWATER PORT ASSESSMENT (IUPA).]*

5532 (U) Radiation/Nuclear Detection (RAD/NUC) Detection Concept of Operations (CONOP) and Standard Operating Procedures (SOP)

[THE COTPS/FMSCS MAY BE REQUESTED TO FACILITATE AND ASSIST THE DEPARTMENT OF HOMELAND SECURITY'S DOMESTIC NUCLEAR DETECTION OFFICE (DNDO) IN THE DEVELOPMENT OF RADIATION/NUCLEAR DETECTION (RAD/NUC) CONCEPT OF OPERATIONS (CONOP) AND STANDARD OPERATING PROCEDURES (SOP) FOR CERTAIN PORT AREAS. RAD/NUC PLANS ARE

ANTICIPATED TO EXTEND BEYOND THE SCOPE OF AMSPS. ACCORDINGLY, THE AMSC/AMSP PLAY SUPPORTING ROLES TO THE AGENCIES RESPONSIBLE FOR DEVELOPING AND EXECUTING RAD/NUC EFFORTS. COTPS/ FMSCS MAY, IN CONSULTATION WITH AMSCS, USE THE AMS PLANNING PROCESS TO FACILITATE CONOP DEVELOPMENT FOR MTS-RELATED RAD/NUC THREATS.

IF A RAD/NUC CONTINGENCY PLAN OR PROTOCOL HAS BEEN DEVELOPED FOR THE COTP AOR OR FOR CERTAIN PORTS WITHIN THE AOR, INCORPORATE IT BY REFERENCE HERE.

IF A CONOP OR PROTOCOL HAS NOT BEEN DEVELOPED, THEN INSERT THE FOLLOWING PLACEHOLDER TEXT: RADIATION/NUCLEAR (RAD/NUC) DETECTION CONCEPT OF OPERATIONS (CONOP) AND STANDARD OPERATING PROCEDURES (SOP) MEASURES, WILL BE COORDINATED BY THE COTP WITH APPROPRIATE AGENCIES USING EXISTING FEDERAL INTERAGENCY DECISION-MAKING AND COORDINATION PROTOCOLS. THE COTP/FMSC WILL FACILITATE RAD/NUC ACTIVITIES FOR MTS-RELATED RAD/NUC THREAT AND CONSULT WITH THE AMSC AS APPROPRIATE TO THE SITUATION.]

5600 (U) Transportation Security Incident (TSI) Management.

[CHARACTERIZE A PLAUSIBLE EXAMPLE(S) OF A TSI EVENT FOR THE PORT/REGION COVERED BY THIS PLAN AND PROSPECTIVE EFFECTS. PROVIDE A SUMMARY OF THE GENERAL MANNER IN WHICH THE INCIDENT WILL BE MANAGED. SUGGESTED CUT AND PASTE CORE TEXT IS SHOWN BELOW.]

5610 (U) Incident Management.

(a) (U) Engagement of pertinent stakeholders should begin as soon as possible following a TSI or threat of a TSI. If an incident occurs without warning, incident management will be initiated using processes, communications procedures and protocols in effect at the time of the incident (i.e., "steady-state operations"). Incident Management will be supplemented by implementation of AMS security response procedures and available first response and contingency plans by the plan owner(s) or by parties designated in the individual plans as appropriate to the situation. Responding organizations will transition to a unified command structure as appropriate when the situation stabilizes sufficiently to enable the transition without loss of incident management continuity.

5620 (U) Procedures for Notification.

(a) (U) All notifications will be carried out using the communication protocols and procedures identified in Section 3400 of this AMSP.

(b) (U) [The contact list is located in Section 3400 or as an appendix to this plan. Identify the location.]

5630 (U) Incident Command Activation.

[THIS SECTION OF THE AMSP WILL ADDRESS THE STEPS NECESSARY TO ACTIVATE A CRISIS MANAGEMENT COMMAND OPERATIONS CENTER SUPPORTED BY ESTABLISHED MEMORANDUMS OF UNDERSTANDING (MOU).]

(a) (U) The COTP/FMSC, normally in consultation with partner agencies, will determine whether there is a need to establish a Unified Command for a particular incident. If established, the Unified Command will follow the guidance and procedures in the National Response Framework (NRF) and National Incident Management System (NIMS) for the Incident Command System (ICS).

(b) (U) Effects of a major TSI or MTS incident outside of the AMS area might impact port operations and security within the area covered by this Plan. Additional maritime security measures and support may be necessary as diverted cargo is processed through the AMS area. The COTP/FMSC may consult with partner agencies regarding the establishment of a Unified Command to support the increased tempo of operations and security measures.

(c) (U) Incident Command Activation Procedures. *[INSERT LOCAL ACTIVATION PROCEDURES.]*

5640 (U) Incident Commander.

(a) (U) The COTP has lead federal responsibility for determining restrictions on port operations, and authorizing movement of vessels, during and following an emergency affecting the port community.

(b) (U) As required by the SAFE Port Act of 2006 (Public Law 109-347, Section 108 (d)) during a TSI within or adjacent to

the jurisdiction of the U.S., the COTP in a maritime security command center (e.g., Interagency Operations Center, Incident/Unified Command Posts) shall act as the Incident Commander, unless otherwise directed by the President.

5650 (U) Pre-Incident Action Plans (optional).

[PRE-INCIDENT IAP TEMPLATES MAY BE DEVELOPED, ADAPTED, AND APPLIED AS AVAILABLE AND APPROPRIATE TO THE INCIDENT INSOFAR AS POSSIBLE. IF ADDED, IAPS SHOULD BE INCORPORATED BY REFERENCE.]

5660 (U) Marine Transportation System (MTS) Recovery Unit (MTSRU).

(a) (U) To facilitate the recovery of the MTS following a TSI, the Coast Guard has adopted inclusion of the MTSRU in the planning section of an IC/UC organizational structure outlined in the Marine Transportation System Recovery Planning and Operations, COMDTINST 16000.28 (series). The MTSRU roles and responsibilities during an incident are identified in the USCG's Incident Management Handbook, COMDTPUB P3120.17 (series), and in the MTS Recovery Plan (MTSRP) for the [*INSERT COTP ZONE NAME HERE*]. The MTSRP will be promulgated, maintained, and made available by request.

(b) (U) The MTSRU will be established as quickly as possible by the COTP/FMSC in response to incidents (i.e., TSI) causing a major disruption to the MTS. The MTSRU is available to identify and populate the Essential Elements of Information (EEI) using the Coast Guard's Common Assessment and Reporting Tool (CART) designed to support MTS recovery decision making and reporting.

(c) (U) The procedures addressing the MTSRU are contained in the MTSRP for the [*Insert COTP Zone Name Here*].

5670 (U) Procedures for Establishing the MTSRU.

(a) (U) The procedures for establishing the MTSRU are contained in the MTSRP for the [*Insert COTP Zone Name Here*].

5680 (U) Measures required prior to initiating MTS Recovery.

(a) (U) The measures required prior to initiating MTS recovery is contained in the MTSRP for the [*Insert COTP Zone Name Here*].

6000 (U) PROCEDURES TO FACILITATE RECOVERY OF THE MARINE TRANSPORTATION SYSTEM (MTS) AFTER A TSI.

[*THE AMSP PROVIDES PLAN ELEMENTS SUPPORTING RECOVERY OF THE MTS AFTER A TSI. THE MTS RECOVERY PLAN (MTSRP) REFERENCED IN THIS SECTION PROVIDES THE ALL-HAZARD APPROACH FOR RESPONDING DISRUPTIONS TO THE MTS TO INCLUDE THE PROCEDURES TO FACILITATE RECOVERY OF THE MTS AFTER A TSI. MTS RECOVERY RELIES ON THE ICS PROCESS FOR PLANNING AND CONDUCTING ACTUAL RECOVERY OPERATIONS DESCRIBED IN THE MTSRP.]*

[THIS SECTION OF THE AMSP ADDRESSES THOSE PROCEDURES FOR RESTORING THE MTS AND THE RAPID FLOW OF TRADE FOLLOWING A TSI, OR THREAT OF A TSI, WHICH COULD INCLUDE IMPLEMENTATION OF INCREASED MARSEC LEVEL 1 SECURITY MEASURES OR THOSE MEASURES EXECUTED DURING MARSEC LEVEL 2 OR LEVEL 3 OUTLINED IN OTHER SECTIONS OF THE AMSP.]

6100 (U) Introduction.

(a) (U) The AMSP for the [*Insert COTP Zone Name Here*] includes procedures to facilitate recovery of the MTS after a TSI. This plan takes into consideration that MTS disruptions may be caused by a TSI, which might directly interrupt normal port rhythm, including cargo operations, vessel movement, and physical security capabilities.

6200 (U) Facilitate MTS Recovery

(a) (U) Procedure. A TSI could produce a capacity constrained event requiring recovery procedures used to deter and mitigate the effects of a TSI. Those procedures correspond with the practices put in place for other categories of MTS disruptions outlined in the MTSRP for the [*Insert COTP Zone Name Here*]. Our MTSRP is designed to provide the necessary procedures that facilitate the safe, efficient, expeditious return of the MTS to its pre-disruption condition.

(b) (U) Requirement. MTS Recovery is included as an element of the AMSP pursuant to the requirements of 33 C.F.R. Part 103. It includes procedures for MTS recovery and requirements of the SAFE Port Act of 2006 to include a Salvage Response Plan, as well as the Coast Guard Authorization Act of 2010 to include area-wide response and recovery protocols to prepare for, respond to, mitigate against, and recover from a TSI. The COTP/FMSC role focuses on coordination of response and recovery procedures and reporting on

the status of the MTS. It does not impact responsibility for the restoration of commercial or private infrastructure, functions, or services.

(c) (U) Facilitate MTS Recovery Concept. The AMSP identifies and relies on existing authorities, funding mechanisms, and capabilities of stakeholders and others. The Plan supports the development of IAPs when MTS recovery operational planning becomes necessary to return the MTS to its pre-disruption operational status. The objective is to ensure that restricted ports and waterways are reopened and the flow of maritime commerce is reestablished as efficiently and effectively as possible. It also provides for a coordinated, stakeholder supported approach for restoring the basic function of the MTS described in our MTSRP.

6300 (U) MTS Recovery Planning and Preparedness.

(a) (U) The MTS recovery planning and preparedness protocols used to facilitate the recovery of the MTS following a TSI is included in the MTSRP for the [*Insert COTP Zone Name Here*].

6400 (U) MTS Recovery Management.

(a) (U) The MTS recovery management protocols used to facilitate the recovery of the MTS following a TSI is included in the MTSRP for the [*Insert COTP Zone Name Here*].

6500 (U) Salvage Response Plan.

[*THIS PLAN ELEMENT ADDRESSES THE SALVAGE RESPONSE PLAN (SRP) REQUIRED BY THE SAFE PORT ACT OF 2006. THE SRP IS A SUPPORTING PLAN TO THE MTS RECOVERY PLAN AS DESCRIBED IN SECTION 6000. PRELIMINARY PLANNING TO ADDRESS OBSTRUCTIONS TO WATERWAYS AND OTHER SYSTEMS CAUSING A DISRUPTION TO THE MTS ARE TASKS THAT ARE DEEMED APPROPRIATE DURING IMPLEMENTATION OF THE MTSRU DESCRIBED IN THE MTSRP AND CG POLICY.]*

[THE SCOPE OF THE SRP IS MARINE SALVAGE AND SIMILAR SERVICES NEEDED TO MITIGATE IMPEDIMENTS TO SAFE NAVIGATION FOLLOWING A TSI OR OTHER CATEGORIES OF MTS DISRUPTIONS DESCRIBED IN THE MTSRP. AS SUCH, THIS PLAN IS INTENDED TO CONCURRENTLY SUPPORT SALVAGE RESPONSE OPERATIONS AND MARINE SERVICES FOR OTHER TRANSPORTATION DISRUPTIONS ACROSS ALL HAZARDS.]

[THE COTP/FMSC SHOULD USE THE TEMPLATE IN ENCLOSURE (6) TO NVIC 09-02 (SERIES) AS THE SRP. THE SRP MUST BE INCLUDED IN THE AMSP AS AN ANNEX TO ENSURE ACCESS AND USE DURING ACTIVATION OF AN INCIDENT MANAGEMENT ORGANIZATION. BASED ON A TSA/USCG DETERMINATION, THE SRP DOES NOT CONTAIN SSI MATERIAL. THEREFORE, THE SRP DOES NOT NEED TO BE MARKED AS SUCH. THE SRP TEMPLATE IS INTENDED TO PROMOTE CONSISTENCY NATIONWIDE ADDRESSING THE CORE ELEMENTS OF SALVAGE RESPONSE WHILE ALSO PROVIDING FLEXIBILITY TO THE COTP/FMSC AND THEIR RESPECTIVE AMSCS WITH ADDRESSING LOCAL SALVAGE RESPONSE NEEDS.]

[LOCAL SALVAGE AND MARINE SERVICES CONTACT INFORMATION, CAPABILITY, AND RESOURCE LISTS SHOULD BE INCLUDED AS TABS TO THE SRP. THE SALVAGE RESPONSE PLANNING ELEMENT WITHIN AN AREA CONTINGENCY PLAN (ACP) SHOULD BE INCORPORATED BY REFERENCE IN THE SRP, BUT IS NOT A SUBSTITUTE FOR INCLUDING AN SRP AS AN ANNEX TO THE AMSP.]

[AT A MINIMUM, THE FOLLOWING TEXT SHALL BE INCLUDED IN SECTION 6500 OF THE AMSP.]

(a) (U) Introduction. The SRP is included as a Plan element within the AMSP pursuant to the SAFE Port Act of 2006. The SRP is normally implemented following disruptions to the MTS, to include disruptions caused by a TSI, resulting in obstructions to waterways or other systems within the MTS contributing to the disruption of the MTS requiring salvage response operations to address restrictions to safe navigation.

(b) (U) Applicability. The SRP for the [*Insert COTP Zone Name Here*] is included as Annex 10200.

(c) (U) Purpose. The purpose of the SRP is to ensure that navigable waterways are cleared of wrecks, obstructions and similar obstacles to allow for the safe and secure transportation of maritime commerce, and that those incidents that disrupt the MTS are mitigated as addressed in the MTSRP.

(d) (U) Compatibility to AMSP and Other Contingencies. When implemented, the SRP is designed to be compatible with the guidance contained within the AMSP used to deter and mitigate the effects of a TSI. The SRP is also designed to be compatible with all other categories of MTS disruptions described in our all-hazard MTSRP.

Therefore, the SRP is used to help guide operational response planning decision making to assist with salvage response, particularly in those cases where salvage resources are needed to support removal of multiple obstructions as necessary.

(e) (U) General Content.

(1) The SRP provides a deliberate planning coordination and procedural framework for conducting salvage operations using existing marine salvage authorities and resources. The Plan identifies and relies on exiting authorities and funding mechanisms of federal agencies and stakeholders with a marine salvage or marine services nexus. The SRP also supports unity of effort when marine salvage response operations become necessary to support the resumption of trade during an incident causing a disruption of the MTS.

(2) The SRP identifies local marine salvage resources and equipment capable of being used to remove waterway obstructions. The Plan also identifies and discusses the use of national salvage capabilities.

(3) The SRP identifies the role of the AMSC and other stakeholders to provide advice and support to decision makers during incidents resulting in marine obstructions to safe/secure navigation.

(f) (U) Salvage Response Concept. The SRP contains planning and preparedness procedures used to support the COTP/FMSC and their respective AMSC with operational salvage response considerations up to the point where incident-specific operational planning is being used to address salvage of marine obstructions to waterways and other systems causing a disruption to the MTS.

(1) (U) When an IC/UC is established, the SRP becomes a supporting plan for salvage response operations and support recovery operational planning decision making during incidents causing a disruption to the MTS. If established, the MTSRU will be tasked with coordinating salvage response activities with other incident management functions such as Planning and Operations where those actions support recovery of the MTS as outlined in the MTSRP.

(2) When an IC/UC is established, salvage response operations will be conducted by individual organizations consistent with their jurisdiction, authorities, funding sources, and capabilities.

(3) Salvage response operations that extend beyond the scope of the SRP will be referred to the established IC/UC for consideration, as appropriate.

7000 (U) [RESERVED]

8000 (U) AREA MARITIME SECURITY PLAN AND ASSESSMENT SYSTEM MAINTENANCE.

[COMDTINST 16601.28 (SERIES) REQUIRES THE COTP/FMSC TO DIRECT, ASSIST AND COORDINATE WITH THE AMSC WITHIN THEIR AREA OF RESPONSIBILITY TO FULFILL THE AMSC'S REQUIREMENTS PURSUANT TO 33 C.F.R. PART 103 AND TO CONDUCT AN ANNUAL EVALUATION AND A DETAILED REVIEW OF THEIR AMSP. PART OF THE PLAN DEVELOPMENT AND MAINTENANCE PROCESS REQUIRES THAT A RISK BASED ASSESSMENT BE CONDUCTED TO ENSURE IDENTIFICATION OF THREATS, VULNERABILITIES AND CONSEQUENCES WITHIN THE AREA OF RESPONSIBILITY. IN ORDER TO PROPERLY CONDUCT AN ANNUAL EVALUATION AND FIVE-YEAR REVIEW OF THE AMSP, THE SOURCE INFORMATION USED TO DEVELOP THE AMSP (I.E., THE AMS ASSESSMENT AND REPORT) MUST ALSO BE REVIEWED FOR CURRENCY, ACCURACY AND COMPLETENESS. THIS SECTION PROVIDES RECOMMENDED LANGUAGE THAT CAN BE USED IN THE PLAN BY THE COTP/FMSC, IN CONSULTATION WITH THE AMSC, TO ESTABLISH BASELINE PROCEDURES AND TIMELINES FOR THE FORMAL AND INFORMAL REVIEW, AMENDMENT, VALIDATION, AND APPROVAL OF THE AMS ASSESSMENT AND THE AMSP.]

(a) (U) This section establishes baseline procedures and timelines for the formal and informal review, amendment, validation and approval of this AMSP and AMS Assessment. [*THE COTP/FMSC IS ENCOURAGED TO ESTABLISH ADDITIONAL PROCEDURES IF NECESSARY TO ENSURE THAT THERE IS A ROBUST REVIEW PROGRAM TO MAINTAIN A DESIRED LEVEL OF ACCURACY AND PREPAREDNESS*].

8100 (U) Procedures for the Regular Review and Maintenance of the AMS Assessments.

(a) (U) The AMSC will ensure that a risk based AMS Assessment is completed and meets the requirements specified in 33 C.F.R. § 103.310 and § 101.510, incorporating the elements specified in 33 C.F.R. § 103.405. AMS Assessments can be completed by the COTP/FMSC, the AMSC, a Coast Guard Port Security Resiliency Assessment team, or by another third party approved by the AMSC.

(b) (U) Five-year Area Maritime Security Assessment.

(1) (U) At least every five years, the COTP/FMSC and the AMSC will ensure that a formal AMS Assessment for their entire Area of Responsibility (AOR) is conducted IAW the requirements and provisions set forth in 33 C.F.R. § 101.510, § 103.310, § 103.405, § 103.410 and COMDTINST 16601.28 (series).

(2) (U) Prior to the start of the AMS assessment, the COTP/FMSC and AMSC will review any prior security assessments, reviews

and relevant reports (Port Security Resiliency Assessments (PSRA), State of the Port reports, MSRAM data updates, AMS assessment validation reports, other government/military port specific assessments, etc.) conducted within their AOR during the previous year. Lessons learned or "best practices" from exercises or real world operations that could impact the AMS assessment will also be reviewed. The purpose of this in-depth review will be the identification of items and issues to be incorporated into the five-year AMS Assessment.

(3) (U) Upon completion of the AMS Assessment, a written report that complies with the requirements of 33 C.F.R. § 103.400 will be included in section 9500 and a summarization of the assessment should be placed in section 3310 of the AMSP.

(4) (U) The AMS Assessment will be completed with sufficient time to ensure that any changes or updates required by the Assessment are incorporated in the five-year submission of the AMSP.

(c) (U) Annual Validation (Informal Review) of the Area Maritime Security Assessment.

(1) (U) At a minimum, the AMS Assessment will be evaluated at least annually to ensure its adequacy, accuracy, consistency, and completeness. This informal review does not relieve the AMSC of their responsibility to develop a process to continually evaluate overall port security by considering consequences and vulnerabilities, how they change over time, and what additional mitigation strategies can be applied. The purpose of the annual assessment validation is to identify gaps in security, verify that threats within the AOR have been evaluated, and to ensure that the vulnerability and consequence assessments for each target/scenario combination remain accurate.

(2) (U) Prior to conducting the AMS Assessment annual validation, the COTP/AMSC will review any prior security assessments and reports (PSRAs, State of the Port reports, MSRAM review updates, etc.) conducted within the previous year in the AOR. Relevant issues contained in other security assessments or reports should be further reviewed for incorporation (informal update) in the AMS Assessment. Changes in infrastructure or operations in the AOR should be reviewed and included in the AMS Assessment if deemed appropriate. Lessons learned from exercises or real-world operations that could result in an

amendment or update to the current AMS assessment will also be reviewed.

(3) (U) Annual reviews of the AMS Assessment will be completed prior to the annual validation of the AMSP and subsequent initial planning phase of the annual Area Maritime Security Training and Exercises Program (AMSTEP) exercise.

(4) (U) Minor amendments or updates to the AMS Assessment do not require a formal review by the Plan Review and Approval Authorities. However, the COTP/FMSC must inform the Plan Review and Approval Authorities when amendments or updates are made.

(d) (U) Immediate Changes of the Area Maritime Security Assessment.

(e) (U) Immediate changes/updates to the AMS Assessment may be appropriate as a result of new threats, formal intelligence, and changes in cargoes or port/facility operations. In those circumstances, COTPs/FMSCs should follow the same procedures described in Section (b) above.

8200 (U) Procedures for the Regular Review and Maintenance of the AMSP.

8210 (U) Five-year Review and Approval of the Area Maritime Security Plan.

(a) (U) A formal update of the AMSP will be performed at least once every five years. Changes in AMSP content requirements may, at times, necessitate an update to or amendment of the Plan within a shorter interval.

(b) (U) Per MTSA, every five years, the COTP/FMSC, with the advice and assistance from the AMSC, will conduct a formal detailed review of the AMSP. This formal review should focus on any change in policy and guidance and on the results of the five-year Area Maritime Security Assessment and determine how the results of the assessment impact the current AMSP. In particular, the COTP/FMSC and AMSC should ensure that changes in cargoes, port infrastructure, and critical port operations are reflected in the Plan.

(1) (U) Once the AMSP has been reviewed by the AMSC, the COTP/FMSC will discuss the findings from the

assessment with the AMSC, and any recommendations from the AMSC regarding amending or updating the Plan.

(2) (U) The COTP/FMSC will ensure that the amended/updated plan is forwarded to the Plan Review Authority (i.e., cognizant Coast Guard District Commander) for review.

(c) (U) The Coast Guard District Commander, as the AMSP Reviewing Authority will coordinate with the COTP/FMSC pursuant to 33 C.F.R. § 103.510 to ensure that any changes or amendments recommended by the District are completed and posted. The District Commander will complete the review of the plan and will forward it pursuant to 33 C.F.R. § 103.510 to the Coast Guard Area Commander (the AMSP Approving Authority) for review and approval.

8220 (U) Annual Validation of the AMSP.

(a) (U) The COTP/FMSC and the AMSC will evaluate the AMSP at least annually for adequacy, accuracy, consistency and completeness. The purpose of this informal review is to ensure that the AMSP has incorporated any relevant and appropriate changes/updates resulting from the Annual Validation of the Area Maritime Security Assessment, lessons learned from exercises and real world operations, and legislative, presidential or policy direction.

(b) (U) Annual validation of the AMSP should be completed prior to the initial planning phase of the annual AMSTEP exercise. This is to ensure that the AMSTEP exercise scenario is developed using the most accurate information available.

(c) (U) Minor amendments or updates to the plans do not require formal review by the Districts or Areas. However, the COTP/FMSC must inform Plan Review and Approval Authorities when changes occur.

8230 (U) Immediate Changes to the AMSP.

(a) (U) There may be occasions for immediate changes to the AMSP. The following are some examples of information that would warrant an immediate change:

(1) (U) Change of emergency points of contact by name and number;

(2) (U) Changes that alter the communications or notification plan;

(3) (U) Changes in jurisdictional or response capabilities;

(4) (U) Physical changes that alter critical infrastructure, operations or avenues of access to the port; or

(5) (U) New threat(s); formal intelligence.

(6) (U) For immediate changes to the plan, the COTP/FMSC will follow the same procedures as for the annual validation as noted in Section 8220 above.

(b) (U) Immediate AMSP Program Wide Plan Review.

(c) (U) When mandates are given dictating the need for an immediate program wide AMSP review and update, they may not be aligned with the existing AMSP formal five-year review and approval cycle. Realizing that these mandated reviews/updates may require approval from the Coast Guard Area Commander as the AMSP Approving Authority, the five-year review and approval clock may be restarted by the AMSP program manager (CG-FAC).

9000 (U) APPENDICES [Required and optional as indicated].

[AN APPENDIX CONTAINING A GLOSSARY IS REQUIRED. SEE ENCLOSURE (7) FOR GLOSSARY OF TERMS AND DEFINITIONS. OTHER APPENDICES ARE OPTIONAL AT THE DISCRETION OF THE COTP/FMSC AND AMSC. USE OF APPENDICES IS SUGGESTED FOR PROCEDURES AND CHECKLISTS AS A READY REFERENCE.]

[THE AMSP CONTAINS SOME INFORMATION THAT IS INTENDED TO REACH A BROAD ARRAY OF MARITIME INTERESTS WHILE OTHER PORTIONS OF THE AMSP WILL BE DESIGNATED AS SENSITIVE SECURITY INFORMATION (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 U.S.C. 553 (b). THE FOLLOWING INSTRUCTIONS APPLY.]

[AN APPENDIX TO AN AMSP IS A PART OF THE PLAN. APPENDICES MAY, HOWEVER, BE MAINTAINED SEPARATELY, WHEN THEY CONTAIN SSI INFORMATION.]

[ALL AMSP APPENDICES MUST INCLUDE PARAGRAPH MARKINGS SO THAT THE DESIGNATION OF ALL INFORMATION IN EACH PARAGRAPH IS READILY APPARENT.]

- *[COTPS/FMSCS AND AMSCS ARE ENCOURAGED TO USE APPENDICES FOR SSI INFORMATION, WHERE APPROPRIATE.]*

- *[SSI INFORMATION MAY BE REDACTED FROM AN AMSP. THE REDACTED AMSP MUST BE MARKED AS REDACTED IN ACCORDANCE WITH APPLICABLE REDACTING REQUIREMENTS PRIOR TO DISSEMINATION (SEE SECTION 3500).]*

- *[EXAMPLES OF APPENDICES ARE LISTED BELOW.]*

9100 (U) AMSC Members.

[INSERT INFORMATION TABLES CONTAINING CONTACT AND AGENCY NAMES, PHONE NUMBERS, EMAIL ADDRESSES, AND/OR OTHER SPECIFIC INFORMATION PERTAINING TO COMMITTEE MEMBERS.]

(a) (U) *[DUE TO THE NATURE OF THE INFORMATION CONTAINED IN THIS APPENDIX, SOME INFORMATION MAY BE EXEMPT FROM PUBLIC DISCLOSURE PURSUANT TO 5 U.S.C. § 553. APPLY SECURITY DESIGNATIONS AS APPROPRIATE.]*

9200 (U) Charts and Maps of Port Areas.

[INSERT ANY CHARTS, SATELLITE PHOTOGRAPHS, MAPS, OR OTHER SPATIAL DATA DEFINING THE COTP ZONE BOUNDARIES.]

(a) (U) *[DUE TO THE NATURE OF THE INFORMATION CONTAINED IN THIS APPENDIX, SOME INFORMATION MAY BE EXEMPT FROM PUBLIC DISCLOSURE PURSUANT TO 5 U.S.C. § 553.]*

9300 (U) Port Operations and Infrastructure.

[INCLUDE PORTIONS OF THE AMS ASSESSMENT THAT LIST OR DETAIL CRITICAL PORT OPERATIONS AND/OR INFRASTRUCTURE FOR THE COTP ZONE.]

(a) (U) *[DUE TO THE NATURE OF THE INFORMATION IN THE AMS ASSESSMENT, THIS APPENDIX WILL BE DESIGNATED SSI AND SHOULD BE MAINTAINED SEPARATELY FROM THE AMSP IN ACCORDANCE WITH 49 C.F.R. PART 1520. INCORPORATE THE AMS ASSESSMENT BY REFERENCE HERE IF NECESSARY. A SUMMARY, IF INCLUDED, MUST BE MARKED WITH THE APPROPRIATE SECURITY DESIGNATION.]*

9400 (U) Risk-Based Scenarios.

[INSERT THE RESULTS OF THE RISK-BASED AMS ASSESSMENT THAT PERTAIN TO THE IDENTIFICATION OF THREAT SCENARIOS SPECIFIC TO THE COTP ZONE. (USE INFORMATION DEVELOPED FOR SECTIONS 3310 AND 5500.)]

9500 (U) AMS ASSESSMENT.

[INSERT THE AMS REPORT AS OUTLINED IN SECTION 3310. TAB B TO ENCLOSURE (2) CONTAINS A RECOMMENDED REPORT TEMPLATE].

10000 (U) ANNEXES [Required and Optional as indicated].

[AN AMSP ANNEX IS PART OF THE AMSP, BUT IS PUBLISHED AS A SEPARATE, DOCUMENT OR SUPPORTING PLAN. THE REVIEW AND APPROVAL THAT APPLIES TO AN AMSP ALSO APPLIES TO AN AMSP ANNEX.]

[MARITIME SECURITY ISSUES AND INITIATIVES MAY EMERGE FOR WHICH INCLUSION IN OR ALIGNMENT WITH THE AMSP IS SUGGESTED OR SOUGHT. THE LEVEL OF DETAIL OR ISSUES MAY BE MORE APPROPRIATELY ADDRESSED AS FIELD-GENERATED BEST PRACTICE GUIDES, JOB AIDS, INCIDENT ACTION PLAN TEMPLATES, OR TEMPLATES FOR DETAILED INCIDENT-SPECIFIC OPERATIONS THAT ARE APPROVED LOCALLY (E.G., BY AN INCIDENT COMMANDER OR UNIFIED COMMAND (IC/UC)). ONCE MATERIAL BECOMES AN ANNEX TO THE AMSP, THE COTPS/FMSCS ARE RESPONSIBLE FOR OBTAINING THE NECESSARY REVIEW AND APPROVALS, AND FOR MAINTAINING ALL ANNEXES INCLUDED IN THE AMSP, INCLUDING PORT-SPECIFIC PLANS WITHIN A SPECIFIC COTP ZONE.]

[A MULTI-PARTY PLAN OR OTHER DOCUMENT THAT IS RELEVANT TO AMS AND WHICH IS SPONSORED BY AN ENTITY OTHER THAN THE COAST GUARD MAY BE BEST SUITED FOR THE SCENARIO, AND THEREFORE SHOULD BE INCORPORATED BY REFERENCE.]

[COTPS/FMSCS ARE NOT AUTHORIZED TO EXPAND AMSP CONTENT TO INCLUDE ADDITIONAL ANNEXES WITHOUT THE CONCURRENCE OF THE COMMANDANT (CG-FAC) AS THE AMS PROGRAM MANAGER, WHICH SHOULD BE OBTAINED IN COORDINATION WITH THE APPROPRIATE COAST GUARD DISTRICT AND AREA COMMANDER. THIS GUIDANCE IS NECESSARY TO ENSURE THAT AMSP CONTENT CONFORMS TO 33 C.F.R. PART 103 AND DOES NOT COMMIT THE COAST GUARD, COTP/FMSC, OR AMSC TO OBLIGATIONS OUTSIDE THE SCOPE OF AMS ROLES AND RESPONSIBILITIES. THE FOLLOWING ARE PRE-AUTHORIZED ANNEXES FOR THE AMSP:

- *PORT-SPECIFIC ANNEXES WITHIN A SPECIFIC COTP ZONE; ALL PORT AREAS COVERED BY AN AMSC REGIONAL SUBCOMMITTEE WITHIN THE COTP ZONE MUST BE INCLUDED AS AN ANNEX.*
- *CYBER INCIDENT RESPONSE PLAN;*
- *SALVAGE RESPONSE PLAN;*
- *UNDERWATER TERRORISM PROTECTION PLAN (UTTP) OR EQUIVALENT (E.G., IUPA); AND*
- *PORT EVACUATION PLAN.]*

10100 (U) Cyber Incident Response Plan.

[A CYBER INCIDENT RESPONSE PLAN MAY BE INCLUDED AS AN ANNEX TO THE AMSP AND SHALL BE INCLUDED AS AN ANNEX OR INCORPORATED BY REFERENCE IF ONE OF THE THREE TSI SCENARIOS INCLUDES A CYBERSECURITY TERRORISM THREAT VECTOR. ENCLOSURE (5) TO NVIC 9-02 (SERIES), PROVIDES AN OPTIONAL TEMPLATE THAT MAY BE ADAPTED FOR THIS PURPOSE.]

10200 (U) Salvage Response Plan.

[A SALVAGE RESPONSE PLAN IS REQUIRED AS PART OF THE AMS PLAN BY THE SAFE PORT ACT. THE SALVAGE RESPONSE PLAN IS A SUPPORTING PLAN TO MTS RECOVERY AS DESCRIBED IN SECTION 6000. SALVAGE RESPONSE PLANNING IS CONSIDERED TO BE A TASK THAT IS APPROPRIATE FOR THE MTSRU. COTPS/FMSCS SHOULD POPULATE AND INCORPORATE ENCLOSURE (6) TO NVIC 9-02 (SERIES), AS THE SALVAGE RESPONSE PLAN.]

10300 (U) Underwater Terrorism Preparedness Plan (UTPP).

[A UTPP OR EQUIVALENT (E.G., IUPA), MAY BE INCLUDED AS AN ANNEX TO THE AMSP, AND SHALL BE INCLUDED AS AN ANNEX OR INCORPORATED BY REFERENCE IF ONE OF THE THREE TSI SCENARIOS INCLUDES AN UNDERWATER TERRORISM THREAT VECTOR.]

10400 (U) Port Evacuation.

[PORT EVACUATION PROCEDURES MAY BE INCLUDED AS AN ANNEX TO THE AMSP, FOR EXAMPLE, WHERE A DETAILED PLAN HAS BEEN COORDINATED WITH PORT AND CIVIL AUTHORITIES (SEE ADDITIONAL GUIDANCE CONTAINED IN SECTION 5330).]

AMSP TABS

Tab A: (U) SSI Non-Disclosure Agreement

Tab B: (U) AMS Assessment Report Template

Tab C: (U) Record of Changes/Annual Validation Template

Tab D: (U) COTP Letter of Promulgation

TAB A: Non-Disclosure Agreement

DEPARTMENT OF HOMELAND SECURITY

I, _____, an individual official, employee, consultant, or subcontractor of or to _____ (the Authorized Entity), intending to be legally bound, hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain information, specified below, that is owned by, produced by, or in the possession of the United States Government.

(Signer will acknowledge the category or categories of information that he or she may have access to, and the signer's willingness to comply with the standards for protection by placing his or her initials in front of the applicable category or categories.)

Initials:	**Protected Critical Infrastructure Information (PCII)**

I attest that I am familiar with, and I will comply with all requirements of the PCII program set out in the Critical Infrastructure Information Act of 2002 (CII Act) (Title II, Subtitle B, of the Homeland Security Act of 2002, Public Law 107-296, 196 Stat. 2135, 6 U.S.C. 101 et seq.), as amended, the implementing regulations thereto (6 C.F.R. Part 29), as amended, and the applicable PCII Procedures Manual, as amended, and with any such requirements that may be officially communicated to me by the PCII Program Manager or the PCII Program Manager's designee.

Initials:	**Sensitive Security Information (SSI)**

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of SSI information as cited in this Agreement and in accordance with 49 C.F.R. Part 1520, "Protection of Sensitive Security Information," "Policies and Procedures for Safeguarding and Control of SSI," as amended, and any supplementary guidance issued by an authorized official of the Department of Homeland Security.

Initials:	**Other Sensitive but Unclassified (SBU)**

As used in this Agreement, sensitive but unclassified information is an over-arching term that covers any information, not otherwise indicated above, which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, as amended, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. This includes information categorized by DHS or other government agencies as: For Official Use Only (FOUO); Official Use Only (OUO); Sensitive Homeland Security Information (SHSI); Limited Official Use (LOU); Law Enforcement Sensitive (LES); Safeguarding Information (SGI); Unclassified Controlled Nuclear Information (UCNI); and any other identifier used by other government agencies to categorize information as sensitive but unclassified.

I attest that I am familiar with, and I will comply with the standards for access, dissemination, handling, and safeguarding of the information to which I am granted access as cited in this Agreement and in accordance with the guidance provided to me relative to the specific category of information.

I understand and agree to the following terms and conditions of my access to the information indicated above:

1. I hereby acknowledge that I have received a security indoctrination concerning the nature and protection of information to which I have been provided conditional access, including the procedures to be followed in ascertaining whether other persons to whom I contemplate disclosing this information have been approved for access to it, and that I understand these procedures.

2. By being granted conditional access to the information indicated above, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from

unauthorized disclosure, in accordance with the terms of this Agreement and the laws, regulations, and directives applicable to the specific categories of information to which I am granted access.

3. I attest that I understand my responsibilities and that I am familiar with and will comply with the standards for protecting such information that I may have access to in accordance with the terms of this Agreement and the laws, regulations, and/or directives applicable to the specific c categories of information to which I am granted access. I understand that the United States Government may conduct inspections, at any time or place, for the purpose of ensuring compliance with the conditions for access, dissemination, handling and safeguarding information under this Agreement.

---

4. I will not disclose or release any information provided to me pursuant to this Agreement without proper authority or authorization. Should situations arise that warrant the disclosure or release of such information I will do so only under approved circumstances and in accordance with the laws, regulations, or directives applicable to the specific categories of information. I will honor and comply with any and all dissemination restrictions cited or verbally relayed to me by the proper authority.

5. (a) For PCII - (1) Upon the completion of my engagement as an employee, consultant, or subcontractor under the contract, or the completion of my work on the PCII Program, whichever occurs first, I will surrender promptly to the PCII Program Manager or his designee, or to the appropriate PCII officer, PCII of any type whatsoever that is in my possession.

(2) If the Authorized Entity is a United States Government contractor performing services in support of the PCII Program, I will not request, obtain, maintain, or use PCII unless the PCII Program Manager or Program Manager's designee has first made in writing, with respect to the contractor, the certification as provided for in Section 29.8(c) of the implementing regulations to the CII Act, as amended.

(b) For SSI and SBU - I hereby agree that material which I have in my possession and containing information covered by this Agreement, will be handled and safeguarded in a manner that affords sufficient protection to prevent the unauthorized disclosure of or inadvertent access to such information, consistent with the laws, regulations, or directives applicable to the specific categories of information. I agree that I shall return all information to which I have had access or which is in my possession 1) upon demand by an authorized individual; and/or 2) upon the conclusion of my duties, association, or support to DHS; and/or 3) upon the determination that my official duties do not require further access to such information.

6. I hereby agree that I will not alter or remove markings, which indicate a category of information or require specific handling instructions, from any material I may come in contact with, in the case of SSI or SBU, unless such alteration or removal is consistent with the requirements set forth in the laws, regulations, or directives applicable to the specific category of information or, in the case of PCII, unless such alteration or removal is authorized by the PCII Program Manager or the PCII Program Manager's designee. I agree that if I use information from a sensitive document or other medium, I will carry forward any markings or other required restrictions to derivative products, and will protect them in the same matter as the original.

7. I hereby agree that I shall promptly report to the appropriate official, in accordance with the guidance issued for the applicable category of information, any loss, theft, misuse, misplacement, unauthorized disclosure, or other security violation, I have knowledge of and whether or not I am personally involved. I also understand that my anonymity will be kept to the extent possible when reporting security violations.

8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to the information covered by this Agreement. This may serve as a basis for denying me conditional access to other types of information, to include classified national security information.

9. (a) With respect to SSI and SBU, I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of the information not consistent with the terms of this Agreement.

(b) With respect to PCII I hereby assign to the entity owning the PCII and the United States Government, all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of PCII not consistent with the terms of this Agreement.

---

10. This Agreement is made and intended for the benefit of the United States Government and may be enforced by the United States Government or the Authorized Entity. By granting me conditional access to information in this context, the United States Government and, with respect to PCII, the Authorized Entity, may seek any remedy available to it to enforce this Agreement including, but not limited to, application for a court order prohibiting disclosure of information in breach of this Agreement. I understand that if I violate the terms and conditions of this Agreement, I could be subjected to administrative, disciplinary, civil, or criminal action, as appropriate, under the laws, regulations, or directives applicable to the category of information involved and neither the United States Government nor the Authorized Entity have waived any statutory or common law evidentiary privileges or protections that they may assert in any administrative or court proceeding to protect any sensitive information to which I have been given conditional access under the terms of this Agreement.

11. Unless and until I am released in writing by an authorized representative of the Department of Homeland Security (if permissible for the particular category of information), I understand that all conditions and obligations imposed upon me by this Agreement apply during the time that I am granted conditional access, and at all times thereafter.

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

13. My execution of this Agreement shall not nullify or affect in any manner any other secrecy or non-disclosure Agreement which I have executed or may execute with the United States Government or any of its departments or agencies.

14. These restrictions are consistent with and do not supersede, conflict with, or otherwise alter the employee obligations, rights, or liabilities created by Executive Order No. 12958, as amended; Section 7211 of Title 5, United States Code (governing disclosures to Congress); Section 1034 of Title 10, United States Code, as amended by the Military Whistleblower Protection Act (governing disclosure to Congress by members of the military); Section 2302(b)(8) of Title 5, United States Code, as amended by the Whistleblower Protection Act (governing disclosures of illegality, waste, fraud, abuse or public health or safety threats); the Intelligence Identities Protection Act of 1982 (50 U.S.C. 421 et seq.) (governing disclosures that could expose confidential Government agents); and the statutes which protect against disclosure that may compromise the national security, including Sections 641, 793, 794, 798, and 952 of Title 18, United States Code, and Section 4(b) of the Subversive Activities Act of 1950 (50 U.S.C. 783(b)). The definitions, requirements, obligations, rights, sanctions, and liabilities created by said Executive Order and listed statutes are incorporated into this agreement and are controlling.

15. Signing this Agreement does not bar disclosures to Congress or to an authorized official of an executive agency or the Department of Justice that are essential to reporting a substantial violation of law.

16. I represent and warrant that I have the authority to enter into this Agreement.

17. I have read this Agreement carefully and my questions, if any, have been answered. I acknowledge that the briefing officer has made available to me any laws, regulations, or directives referenced in this document so that I may read them at this time, if I so choose.

DEPARTMENT OF HOMELAND SECURITY

NON-DISCLOSURE AGREEMENT

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

Acknowledgement

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

WITNESS:

Typed/Printed Name:	Government/Department/Agency/Business Address	Telephone Number:

This form is not subject to the requirements of P.L. 104-13, "Paperwork Reduction Act of 1995" 44 U.S.C., Chapter 35.

TAB B: Area Maritime Security Assessment Report Template

AREA MARITIME SECURITY ASSESSMENT REPORT {33 C.F.R 103.400}

1. (U) Name of COTP Zone:

_____

2. (U) The Area Maritime Security Assessment was conducted by *[INSERT NAME OF PERSON(S), TEAM, AND/OR THIRD PARTY CONDUCTING THE ASSESSMENT]* incorporating data analysis from multiple sources to include MSRAM data analysis by the COTP/AMSC {Recommend to use AMSA Job Aid}.

3. (U) Summary of Assessment methodology, to include a list of the past security assessments (title and date) that have informed this assessment:

_____
_____
_____
_____
_____
_____

4. (U) Types **of maritime operations conducted in the COTP Zone**: (i.e., HCPV, CDC, HVU, Chemical, Container, Bulk, Break Bulk, Cyber, etc.)

_____
_____
_____
_____
_____
_____
_____
_____

VULNERABILITY & SECURITY MEASURES

5. ( ) Vulnerability/Consequence (brief description):

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

5. a. ( ) MARSEC Level I Risk Reduction Strategies:

5. b. ( ) MARSEC Level II Risk Reduction Strategies:

5. c. ( ) MARSEC Level III Risk Reduction Strategies:

6. ( ) Vulnerability/Consequence (brief description):

6. a. ( ) MARSEC LEVEL I Risk Reduction Strategies:

6. b. ( ) MARSEC Level II Risk Reduction Strategies:

6. c. ( ) MARSEC Level III Risk Reduction Strategies:

7. ( ) Vulnerability/Consequence (brief description):

7. a. ( ) MARSEC Level I Risk Reduction Strategies:

7. b. ( ) MARSEC Level II Risk Reduction Strategies:

7. c. ( ) MARSEC Level III Risk Reduction Strategies:

8. ( ) Vulnerability/Consequence (brief description):

8. a. ( ) MARSEC Level I Risk Reduction Strategies:

8. b. ( ) MARSEC Level II Risk Reduction Strategies:

_____
_____
_____
_____
_____
_____
_____

8. c. ( ) MARSEC Level III Risk Reduction Strategies:

_____
_____
_____
_____
_____
_____
_____

AMSA SIGNATURE PAGE
(Signature/Date)

Approved:	_____	_____
	COTP/FMSC	AMSC Chairperson
Annual Validation:	_____	_____
	COTP/FMSC	AMSC Chairperson
Annual Validation:	_____	_____
	COTP/FMSC	AMSC Chairperson
Annual Validation:	_____	_____
	COTP/FMSC	AMSC Chairperson
Annual Validation:	_____	_____
	COTP/FMSC	AMSC Chairperson

TAB C: AMSP Record of Changes/Annual Validation

AMSP Record of Changes/Annual Validation			
CHANGE NUMBER	DATE OF CHANGE/VALIDATION	PAGES AFFECTED	BY WHOM ENTERED

TAB D: Area Maritime Security Plan (AMSP) Letter of Promulgation Template

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

[COTP]
United States Coast Guard

[STREET ADDRESS]
[LOCATION, STATE]
Staff Symbol
Phone:
Fax:

16601
[DATE]

From: Captain of the Port _____
To: Distribution

Subj PROMULGATION OF _____ AREA MARITIME SECURITY PLAN

1. This letter promulgates the *[INSERT YEAR]* update to the _____ Area Maritime Security (AMS) Plan covering Captain of the Port (COTP) _____ Zone *[OR AMS AREA IF THE AMS PLAN COVERS A SUBSET OF THE COTP ZONE]*. This AMS Plan is effective this date, and remains in effect until otherwise notified by the COTP.

2. The COTP, serving as the designated Federal Maritime Security Coordinator (FMSC) pursuant to 33 C.F.R. § 103.200, developed this Plan in consultation with the _____ Area Maritime Security Committee as required by 33 C.F.R. § 103.500. This Plan is for use by the COTP/FMSC, the _____ AMS Committee; federal, state, local, territorial, and tribal governments; and other AMS partners and stakeholders. The structure of the AMS Committee, its relationship with the FMSC, and its role in AMS planning are described in the committee charter.

3. This Plan was developed under the authority of Section 102 of the Maritime Transportation Security Act of 2002 (MTSA), Public Law 107-295, codified at 46 U.S.C. 70101-70117, which mandates the development of an Area Maritime Transportation Security Plan. It includes a Salvage Response Plan pursuant to the requirements of Section 101 of the Security and Accountability for Every Port Act of 2006 (SAFE Port Act), Public Law 109-347. It also includes response and recovery protocols to prepare for, respond to, mitigate against and recover from a transportation security incident pursuant to the requirements of Section 826 of the Coast Guard Authorization Act of 2010.

4. This Plan implements its AMS Area applicable provisions of the International Ship and Port Facility Security (ISPS) Code by including content required by 33 C.F.R. § 103.505, as elaborated by the NVIC No. 09-02, series, Guidelines for Development of Area Maritime Security Committees and Area Maritime Security Plans Required for U.S. Ports.

5. Plan content covers prevention, protection, security response, and facilitated recovery of the Marine Transportation System (MTS) from transportation security incidents (TSI), regardless of specific cause, size or complexity. Content of the MTS Recovery Plan is designed for all-hazard compatibility relative to other categories of transportation disruptions, as defined by MTSA and the SAFE Port Act, insofar as practicable. It provides a maritime security baseline for routine prevention activity, and guides transition from day-to-day activities through implementation of organization-specific contingency and response plans to implementation of unified incident management. *[OPTIONAL: POINTS OF EMPHASIS MAY BE INCLUDED AT COTP/FMSC DISCRETION. SUGGESTED GENERIC TEXT IS SHOWN IN ITALICS.] This AMS Plan:*

    a. *Provides a port-level framework for a unified and coordinated approach to maritime security preparedness and domestic maritime security incident management;*

    b. *Complements required facility and vessel security plans, and develops strategies to ensure appropriate protection of those vessels, facilities and port infrastructure that are not regulated under 33 C.F.R. Parts 104, 105, and 106;*

    c. *Outlines general AMS partner and stakeholder responses to changes in Maritime Security (MARSEC) Levels;*

    d. *Identifies joint measures and procedures to encourage and guide mutually supporting maritime security activity throughout the AMS area;*

    e. *Provides linkages to contingency, response and similar plans, including the Area Contingency Plans (ACP).*

    f. *Serves as a Concept Plan (CONPLAN) under the National Response Framework (NRF) for informing the maritime component of incident management when National Incident Management System (NIMS) structures are implemented at the port level.*

6. Portions of this Plan are designated and marked as Sensitive Security Information (SSI). This Plan shall be safeguarded from unauthorized disclosure of SSI information pursuant to 49 C.F.R. Part 1520. Administration of SSI will observe the guidance contained in NVIC No. 10-04, Guidelines for Handling of Sensitive Security Information (SSI), COMDTPUB P16700.4.

7. This AMS Plan is a living document and will continue to evolve, reflecting lessons learned from application, training, actual operations and exercises. All AMS partners and stakeholders are responsible to ensure that those portions of the Plan which concern their operations and activities are correct and up-to-date, and for drafting and submitting a correction to the Plan. Revisions will be submitted for

approval and promulgation to the COTP/FMSC for consultation with the _____ AMS Committee.

8. Nothing in this Plan shall be construed as contravening or superseding applicable laws or regulations or other directives issued by proper authority. Should any conflict arise between this Plan and any of the foregoing, the COTP shall be promptly advised.

_____

[COTP NAME]
Captain of the Port/Federal Maritime Security Coordinator

ENCLOSURE (3) TO NVIC 9-02 CHANGE 5

AREA MARITIME SECURITY (AMS) ASSESSMENT

AREA MARITIME SECURITY (AMS) ASSESSMENT GUIDANCE

1. AMS Assessment Requirements. The AMS Assessment is an important foundational step in developing and maintaining the Area Maritime Security Plan (AMSP). This enclosure describes the essential elements of an AMS Assessment as described in MTSA implementing regulations. These provisions are consistent with the elements of a "port facility security assessment" set forth in the International Ship and Port Facility Security (ISPS) Code. The AMS Assessment should address port risk across the COTP Zone, with a primary focus on the areas outside the fence lines of individual facilities; however if a terrorist attack could occur within the boundaries of a facility that may result in a Transportation Security Incident (TSI) to the Marine Transportation System (MTS); (e.g., a Certain Dangerous Cargo (CDC) storage facility with inadequate stand-off distances for vehicle-borne improvised explosives may need a barrier system) then the focus should include the facility as a whole.

   a. The Area Maritime Security Committee (AMSC) is required by 33 C.F.R. § 103.400 to ensure that a risk-based AMS Assessment is completed and meets the requirements specified in 33 C.F.R. § 103.310 and 33 C.F.R. § 101.510, incorporating the elements specified in 33 C.F.R. § 103.405. The AMS Assessment can be completed by the COTP, the AMSC, a Coast Guard Port Security Resiliency Assessment Team, or by another third party approved by the AMSC (e.g., contract support). After completion of an AMS Assessment, Section 3310 of the AMSP will summarize the written report which will be inserted in Appendix 9500. This should be designated as Sensitive Security Information (SSI), that complies with the requirements of 33 C.F.R. § 103.400. The report shall include:

      (1) A summary of how the AMS Assessment was conducted;

      (2) A description of each vulnerability and consequence found during the AMS Assessment; and

      (3) A description of risk reduction strategies that could be used to ensure continued operation at an acceptable risk level.

      (4) Tab B to Enclosure 2 of this NVIC contains a sample written report template that may be used when developing the AMS Assessment written report.

   b. The AMS Assessment will be developed and maintained in accordance with the requirements outlined in the Area Maritime Security Plan (AMSP) and Area Maritime Security (AMS) Assessment Development and Maintenance Process, COMDTINST 16601.28 (series).

2. AMS Assessment Elements and Considerations

a. In order to be considered valid, the AMS Assessment must contain the following elements as described in 33 C.F.R. § 103.405:

(1) Identification of the critical Marine Transportation System (MTS) infrastructure and operations in the port (COTP Zone);

(2) Threat assessment that identifies and evaluates each potential threat on the basis of various factors, including capability and intention;

(3) Consequence and vulnerability assessments for each target/scenario combination; and

(4) A determination of the required security measures for the three MARSEC levels.

b. In order to meet the elements listed above, an AMS Assessment should consider each of the following:

(1) Physical security of infrastructure and operations at the port (COTP Zone);

(2) Structures considered critical for the continued operation of the port (COTP Zone);

(3) Existing security systems and equipment available to protect maritime personnel and infrastructure;

(4) Procedural policies;

(5) Radio and telecommunication systems, including computer systems and networks (Examples: Automated Cargo Container Tracking Systems, Shore-based systems, GPS, lock operation, cargo handling systems, “industrial control systems”, etc.).

(6) Relevant transportation infrastructure;

(7) Utilities;

(8) Security systems, resources and capabilities; and

(9) Other areas that may, if damaged, pose a risk to people, infrastructure, or operations within the COTP Zone.

c. Data collection will be required to analyze the elements listed above. The AMSC/COTP shall ensure that a complete site survey of each port area described in the AMSP within the COTP area of responsibility is conducted as part of the AMS Assessment. The port area site survey is a critical, on-site examination used to determine existing security conditions at key components of the port, identify security deficiencies/vulnerabilities and consequences, and develop mitigation strategies to improve security and reduce the risk and consequences of an attack. In conducting the AMS Assessment, the AMSC/COTP shall ensure that the port area site survey results are analyzed to provide recommendations to establish and prioritize the security measures that should be included in the AMSP. This data collection effort requires collaboration and input from local maritime industry port partners, federal, state and local government representatives, as well as expertise from other subject matter experts (e.g., local utilities, transportation authorities).

3. Vulnerability Assessment. The vulnerability of an area, facility, or operation within the port is determined by the likelihood that a terrorist attack would be successful, after consideration of a number of relevant issues. Factors considered in determining vulnerabilities at facilities, vessels, waterways, and infrastructure include the existence and effectiveness of organic layered security systems designed to detect/deter/prevent unauthorized entry (e.g., barriers/fencing, surveillance systems/sensors, lighting, entry control point technology/staffing, computer systems and networks [resilience/protection/procedures, etc.], effectiveness of organic security force, etc.), the "hardness" of facilities/vessels to the effects of an attack (e.g., whether significant damage/disruption would result if a terrorist attack occurred), and the existence/effectiveness of external law enforcement or systems/forces as an additional layer of security beyond the organic security provided by facility, infrastructure, and vessel owners/operators (e.g., police/harbormaster/Coast Guard patrols, harbor surveillance or camera systems). Input for the Vulnerability Assessment process is provided by Coast Guard staffs, Assessment Team personnel, AMSC members, and other subject matter experts.

4. Consequence Assessment

a. The Consequence Assessment is the process of evaluating the impact and effects of a successful terrorist attack [e.g., Active Threat/Shooter] on one or more components of the MTS (e.g., infrastructure, vessels [cargo and passenger], computer systems and networks, and waterways) in a port area. Consequences are derived by considering the target's reasonable worst-case effects with regard to the five factors listed below:

- Casualties (deaths/injuries);

- Economic impacts (both primary and secondary);

- Environmental impact;
- National Security; and
- Symbolic.

b. When considering these factors, the assessor must also consider the mitigation and response capabilities, and capacity of the owner/operator, local first responders, the Coast Guard and other federal agencies, as well as the target's recoverability and redundancy. Coast Guard personnel, along with input from AMSC members, determine the consequences based on historical port knowledge, stakeholder input, and Assessment Team input regarding COTP Zone-wide security measures and response capabilities.

c. When possible, Consequence Assessments should also consider factors not currently considered in existing risk models that could influence the evaluation of the consequence of a successful terrorist attack in a port area. These would include factors such as "cascading effects," which is the ripple effect of an attack on key sectors of the economy, and is derived by determining whether a terrorist attack on a few key assets would have a disproportionate effect across the rest of the MTS in the port.

5. The Recommended AMS Assessment Process

a. AMS Assessment Charter. A written Charter formally establishes the process that will be used to conduct the AMS Assessment. The Charter should provide guidance regarding the purpose/objectives of the AMS Assessment, roles and responsibilities for AMS Assessment Team members (and other participants), and timelines for research, analysis and production of the AMS Assessment Report. The Charter should be approved and signed by the COTP/FMSC and a non-CG member of the AMSC.

b. AMS Assessment Team. The persons conducting the AMS Assessment must have the appropriate skills to evaluate the security of the port in accordance with federal regulations (33 C.F.R. § 103.410). The regulations specify that persons participating in the AMS Assessment be able to "draw upon expert assistance" to complete their task. This approach envisions that subject matter experts and data from a variety of sources and disciplines (from the AMSC and external sources) will be used to develop the AMS Assessment. The persons identified in the Charter as having roles and responsibilities in the development of the AMS Assessment make up the AMS Assessment Team. It is important that the AMS Assessment Team members are selected based on their expertise. The expertise required to complete the assessment will vary from port to port depending upon the specific infrastructure and operations that are conducted within the port.

c. Project Management Plan. A Project Management Plan (PMP) can be developed by the AMS Assessment Team to identify project goals and objectives, the roles and responsibilities of the AMS Assessment Team, contact information for project participants, analysis assumptions and constraints, project phases and timelines, and requirements for deliverables.

d. Data Collection Plan. A Data Collection Plan is used to identify sources, types, and collection methods for information to be considered during the analysis phase of the assessment. A Data Collection Plan may be included in the PMP (in the main body of the document, or as an Appendix), or developed as a separate document. This includes information obtained from visual observation during the site survey of port areas, facilities, critical infrastructure and port operations in addition to information obtained from interviews with port stakeholders, utility providers, and Federal, State and local law enforcement, etc.

e. Analysis. The analysis represents the core of the AMS Assessment, and is informed by the data collected, and framed by the objectives, assumptions and constraints identified in the AMS Assessment Charter and PMP. The analysis should be designed to assess the effectiveness of security measures currently in place in the port, identify security deficiencies, develop mitigation strategies, determine priorities for reducing risk, and provide a basis for requesting or reprogramming resources to mitigate risk.

f. Findings and Recommendations. The Findings and Recommendations in the AMS Assessment are derived from the results of the analysis. During the review, critical MTS infrastructure and port operations are identified, required security measures for all MARSEC levels are determined, and the required TSIs are documented in the AMSP. This step is also where the mitigation strategies are listed for port vulnerabilities identified during the site surveys.

g. AMS Assessment Report. This written report is required by 33 C.F.R. 103.400 and is designated SSI. The AMS Assessment Report must contain the items listed in 1 (a).

6. Further information regarding the phases of the AMS Assessment process, checklists and other guidance for completing the required elements of the assessment, and guidance focused towards improving understanding of the relationship of the assessment elements to each other are contained in the AMS Assessment Job Aid.

7. Use of Other Assessments, Studies, and Plans During AMS Assessments

a. Previous AMS Assessments. Information contained in previous AMS Assessments may still be current, applicable and used during the current

assessment. AMS Assessment Teams are encouraged to conduct a thorough review of previous AMS Assessments and use current and relevant data that complies with the regulatory requirements to inform the development of the AMS Assessment. The information from a prior assessment should be retained with and interwoven into the new assessment. Information obtained from previous assessments must be validated before using to inform the new AMS Assessment (e.g., during the site survey, interviews with subject matter experts, etc.).

b. Port Security Resiliency Assessments (PSRA). Although PSRAs alone do not meet the regulatory requirements of an AMS Assessment, they are a valuable source of information to be considered when developing AMS Assessments. PSRAs provide a very good MARSEC Level I security assessment of specific facilities and waterways within a port. However, PSRAs normally do not include a site survey of the entire port area, nor do they provide mitigation strategies for MARSEC II or III. PSRAs that are current (i.e., when the data and other supporting information has not changed) should be reviewed, and any relevant data used as appropriate to inform the 5 year AMS Assessment.

c. Facility Security Assessments/Plans. The current regulations (33 C.F.R. § 105.415) require that an audit of the Facility Security Plan (FSP) be conducted annually. Facility Security Officers are required to update/amend the Facility Security Assessment (FSA) and FSP if the results of the annual audit indicate that updates or a change is required. Current and accurate information contained in the FSA or FSP can be used to inform the AMS Assessment. (This data should have already been vetted as current and accurate as COTPs are required to approve changes to the FSP or FSA.)

d. Maritime Security Risk Analysis Model. The Maritime Security Risk Analysis Model (MSRAM) has valuable information that can be used to support the development of AMS Assessments. However, MSRAM by itself does not satisfy AMS Assessment requirements and therefore is not considered an AMS Assessment. MSRAM is a tool that is used in the AMS Assessment process. The MSRAM tool can be used to analyze data collected from the field during the site surveys conducted as part of the AMS Assessment process. MSRAM supports the AMS Assessment in the following ways:

(1) The threat data in MSRAM is provided directly by the Intelligence Coordination Center (ICC) for specific combinations of target type, MSRAM attack mode, and geographic location on current intelligence;

(2) MSRAM can (based on the data entered) identify the highest risk scenarios in the port area;

(3) MSRAM analysis (based on the data entered) can assist with identifying the top three risk based TSIs for the port area; and

(4) MSRAM can be used to evaluate mitigation strategies and the risk reduction they provide.

e. Other Assessments, Reports, Plans, Studies, and Data. There are numerous other assessments (e.g., Threat and Hazard Identification Assessment), reports, plans (e.g., Port Wide Risk Management Plan), studies, and data regarding port security that have been developed and completed in ports by applicable local, State, and other Federal entities to support various port security objectives. While developed for other purposes, these products and data sources may contain valuable information that can be used to inform the development of the AMS Assessment. Similar to data obtained from other sources, any information used in AMS Assessments must be both accurate and relevant. Anytime information from another plan, report or study is used to inform the AMS Assessment, the source information and collection methods should be cited (e.g., by reference, footnote/endnote, etc.). Additional guidance regarding information sources and uses to support AMS Assessments is contained in the AMS Assessment Job Aid. Other assessments that meet all of the regulatory requirements for an AMS Assessment may be used and should be documented in section 3 of the AMSA Report.

ENCLOSURE (4) TO NVIC 9-02 CHANGE 5

AREA MARITIME SECURITY EXERCISE PROGRAM GUIDANCE

AREA MARITIME SECURITY TRAINING EXERCISE PROGRAM (AMSTEP) GUIDANCE

REFERENCES:

(a) Navigation and Navigable Waters, Maritime Security: Area Maritime Security, 33 C.F.R. Part 103

(b) Contingency Preparedness Planning Manual Volume III - Exercises, COMDTINST M3010.13 (series)

(c) Coast Guard After Action Program (CGAAP), COMDTINST 3010.19 (series)

(d) Transportation, Security Rules For All Modes of Transportation; Protection of Sensitive Security Information, 49 C.F.R. Part 1520

(e) Navigation and Vessel Inspection Circular No. 10-04, Guidelines for Handling of Sensitive Security Information (SSI), COMDTPUB P16700.4 (series)

(f) Department of Homeland Security, Ports, Waterways, and Coastal Security (PWCS) Security Classification Guide, DHS SCG USCG 001.5 (PWCS), 15 November 2016

1. PURPOSE. This enclosure provides guidance to Coast Guard Captains of the Port (COTPs)/Federal Maritime Security Coordinators (FMSCs) and Area Maritime Security Committees (AMSCs) regarding their responsibilities to conduct exercises to test Area Maritime Security Plans (AMSPs).

2. Directives Affected. Commandant (CG-544) Policy Letter 01-14, Area Maritime Security Training and Exercise Program (AMSTEP) Cycle Change, 05 March 2014 was incorporated in Reference (b).

3. BACKGROUND.

   a. Coast Guard COTPs and AMSCs are required by Reference (a) to ensure that exercises are conducted each calendar year to test the implementation and effectiveness of AMSPs. Flexibility is provided for scheduling exercises within the year, provided that the interval between exercises does not exceed 18 months. These exercises are an indispensable component of the Plan-Organize/Equip-Train-Exercise-Evaluate/Improve preparedness cycle used to continually improve and assess the effectiveness and validity of the AMSP against existing plan requirements, as well as ongoing risk/threat assessments. The exercises are one of the primary tools used to validate information and procedures in the AMSP, identify strengths to share as best practices, and to practice Command and Control (C2) within an Incident Command/Unified Command (IC/UC) framework.

   b. Initial versions of the AMSPs were completed in the spring of 2004, and AMSCs were required to conduct or participate in an Area Maritime Security (AMS) exercise prior to 31 DEC 2005. Subsequent exercises (or credit for actual security preparedness

operations in lieu of exercises) were required to comply with the provisions of Reference (a).

c. The Homeland Security Exercise and Evaluation Program (HSEEP) provides exercise guidance and principals based on national best practices that constitute a national standard for homeland security exercises and have been adopted by the Coast Guard as the standardized policy and methodology for exercises in Reference (b).

4. DISCUSSION.

a. Exercise Policy. This enclosure provides programmatic guidance and expectations specific to planning and conducting AMS exercises.

b. Preparedness. AMS preparedness involves a continuous process that begins with the AMS Assessment, continues with planning and training followed by exercises, which are developed and conducted as a means to determine if the AMSP adequately addresses the maritime security needs of the port. These exercises test protocols, procedures, and measures for prevention, protection, response, and system stabilization and recovery activities to mitigate risk to the Marine Transportation System (MTS) from terrorist threats or acts. Lessons learned are developed for incorporation into AMSP updates, while best practices are shared with other ports as a resource for improving maritime security.

c. Exercise Development. This enclosure, in conjunction with References (b) and (c), will be used to guide the development and execution of the AMSTEP exercises. This alignment allows the AMSTEP to better support partner and stakeholder participation.

d. Regulatory Compliance. As previously noted, Section 103.515 of Reference (a) requires that each AMSP be exercised at least once each calendar year, with the interval between the exercises not exceeding 18 months.

5. AREA MARITIME SECURITY TRAINING AND EXERCISE PROGRAM (AMSTEP).

a. AMSTEP Exercise Alignment. AMSTEP exercises are an integral part of a coordinated, comprehensive national exercise program. Therefore, AMSTEP exercises will align with and support Presidential Policy Directive 8: National Preparedness and its elements, National Maritime Transportation Security Plan (NMTSP), which serves concurrently as the Maritime Modal Annex to the Transportation Systems Sector Specific Plan (TS SSP), National Infrastructure Protection Plan (NIPP), Maritime Infrastructure Recovery Plan (MIRP), and the DHS Strategy to Enhance International Supply Chain Security.

b. AMSTEP Goals. The overall goals are to test the effectiveness of AMSPs, identify areas for improvement, and otherwise support MTSA through effective AMSP implementation. Supporting goals are identified below.

(1) Improve the capability to:

(a) Deter Transportation Security Incidents (TSI);

(b) Implement and conduct coordinated interagency command and control operations in accordance with the National Incident Management System (NIMS);

(c) Communicate effectively with various federal, state, local, tribal, and territorial agencies, as well as industry stakeholders, across all affected modes of transportation (while engaged in the prevention, response, or recovery activities associated with a TSI);

(d) Facilitate sharing, correlating, and disseminating information and intelligence (including Sensitive Security Information (SSI)) among members of the AMSC to prevent or effectively respond to a TSI;

(e) Attain and maintain MARSEC levels as directed;

(f) Implement prevention and protection procedures;

(g) Prepare appropriate stakeholders in the COTP/FMSC Area of Responsibility to respond to and mitigate the adverse effects of a TSI, to include improving linkages to appropriate incident management and response plans; and

(h) Coordinate system stabilization and recovery from a TSI and support restoration of key transportation services and critical infrastructure within the affected port.

(2) Validate:

(a) Identification of security procedures for critical infrastructure within the port; and

(b) TSI planning scenarios.

(3) Ensure the protocols and procedures used to prevent, protect, respond to, and recover from TSIs are compatible with those used for other Transportation Disruptions and contingencies.

c. AMSTEP Exercise Requirements. The following program standards for AMSTEP exercises are intended to provide a nationwide baseline for exercise performance, while also providing flexibility to plan, design, and conduct exercises that best suit the needs of the COTP zone. It is recommended that consideration be given to integrating

AMSTEP exercises with exercises supporting other contingencies or organizations in order to leverage opportunities to meet multiple training or exercise objectives in a single venue.

(1) Annual Exercises. Each AMSP will be exercised at least once each calendar year with no more than 18 months between exercises, in compliance with Reference (a). The AMSP Approval Authority, in consultation with the Coast Guard Headquarters AMSP Program Manager (the Office of Port and Facility Compliance (CG-FAC)), will maintain and publish a current list of AMSPs.

(a) Where a region-wide AMSP has been established and major sub-areas are addressed using subcommittees with geographically defined plan annexes; each geographically defined annex must be exercised at least once every four years. Geographically defined annex subcommittees may choose to exercise more frequently but must ensure visibility of efforts to ensure ability to meet overarching AMSTEP and Multi-Year Training and Exercise Plan (MTEP) coordination intent.

(b) Each port within each AMSP coverage area must be included in an AMSTEP exercise at least once every four years. Ports and port areas that best test the effectiveness of the AMSP should be selected for inclusion in individual exercises. The AMSP Approval Authority is responsible for maintaining a current list of ports or port areas to which this exercise requirement applies.

(c) Either the discussion-based or operations-based exercises, described in Reference (b) may be used to meet the annual exercise requirement as per the cycle. The COTP/FMSC will exercise at least once in the four-year cycle, without raising the MARSEC Level, implementation of enhanced security measures at the MARSEC Level 1 outlined in the AMSP to individual vessels, facilities, or persons. This flexibility addresses emergency security threats in a port and aligns security processes with risks and other considerations. However, at least once during each four-year cycle the AMSTEP exercise must be operations-based (Full Scale or Functional) and include: activation of an Incident Command/Unified Command structure, and should also include an increase in MARSEC Level in response to either a directed change in MARSEC Level by the CG COMDT (e.g., due to a terrorist threat that could result in a TSI), a TSI, or a combination of these contingencies.

(2) Plan Elements Subject to Testing. All main elements of the AMSP identified in Tab A to this enclosure must be exercised not less than the frequency indicated. If an AMSP is updated during the four-year exercise cycle, then the updated element(s) should be validated as soon as possible in an AMSTEP exercise. AMSTEP exercises may be very comprehensive and broad in scope, or may be limited to focus on specific plan elements and associated exercise objectives.

(3) Exercise Objectives. Exercise objectives will be based on the AMSP elements being tested and other needs as determined through the ongoing risk/threat assessments of the COTP/FMSC and AMSCs. A non-inclusive list of sample objectives is contained as Tab B for discretionary use.

(4) Exercise Scenarios.

(a) Exercises must focus on scenarios that involve the threat of a TSI, or a TSI.

(b) Each of the three primary TSI planning scenarios in the AMSP must be exercised at least once during each four-year exercise cycle in an AMSTEP exercise.

(c) MARSEC changes will not be used as exercise scenarios. MARSEC changes are security responses to a TSI (or threat of a TSI), and are not scenarios. For example, a credible threat may necessitate a security response in the form of an increase in the MARSEC level. Restoration of cargo flow would constitute recovery from the threat itself, not from the security procedures imposed in response to the threat.

(5) AMS Exercise Credit for other Exercises and Actual Security Preparedness Operations. Guidance for obtaining and documenting AMS exercise credit is contained in Tab C.

d. AMSTEP Exercise Roles and Responsibilities.

(1) Institutional Roles and Responsibilities.

(a) The Coast Guard Area Commanders (as the AMSP Approving Authority), District Commanders (as the AMSP Reviewing Authority), COTPs/FMSCs and other Coast Guard organization entities are responsible for administering and conducting AMSTEP exercises in conformance with this enclosure.

(b) The Coast Guard will serve as the sponsor of AMSTEP exercises or AMSTEP exercise components of other exercises. Other roles and responsibilities associated with AMSTEP exercises will vary with the scope, scale, and complexity of the exercise, the level of participation by other organizations (e.g., local, regional, national), and other factors.

(c) The Exercise Sponsor, Director, and Planning Team Leader roles are discussed in detail in Reference (b).

(d) The COTPs/FMSCs will normally be responsible for staffing and administration of Exercise Planning Teams. Districts, in their role assisting

program, should provide subject matter expert support for the exercise design and evaluation functions, in cooperation with AMSCs and other port stakeholders.

(2) Preparedness Engagement.

(a) The AMSC will be involved in all phases of the AMS preparedness to ensure that the AMSP and exercises meet stakeholder goals and objectives. Establishment of AMSTEP Exercise Subcommittees is strongly recommended to ensure appropriate focus is given to scheduling, planning, conducting, and evaluating exercises in support of the AMSP and overall port security preparedness efforts. Members of an AMSTEP Exercise Subcommittee, where established, should be well versed in homeland security preparedness doctrine as well as exercise principles.

(b) Training should be conducted on an ongoing basis to enhance and sustain readiness for actual incidents. The AMSC and FMSC should identify training needed to enhance specific knowledge and skills among stakeholders needed to support AMSP elements.

(3) AMSTEP Specific Exercise Planning and Design Considerations. General AMSTEP planning, design, control, conduct and evaluation should be guided by Reference (b). Several factors that should be considered before commencing the exercise planning include, but are not limited to: available funds, available space, geographic or climate considerations, scheduling conflicts/participant availability, last review date of the AMS Assessment and AMSP, exercise requirements, and changes in personnel or stakeholders.

(a) AMS Assessment. The AMSC and COTP/FMSC are responsible for the validation of the AMS Assessment to determine if updates to the AMSP are required. The results of this assessment validation should be used to inform decisions regarding specific plan elements to be tested during a particular AMSTEP exercise. Objectives will then be developed to drive the scope of the exercise, as well as the level of participation.

(b) Readiness of the AMSC and the Port Community. If the AMSP recently underwent a significant update, and the AMSC would benefit from improved familiarity with plan elements, a discussion-based exercise(s) may be the best first step, followed by operations-based exercises. This concept reinforces the training value of exercises and use of a progressive approach to build participant skills, teamwork and familiarity with the plan.

(c) Private Sector Involvement in AMSTEP Exercises.

[1] The AMSP elements included in the exercise objectives will determine the appropriate level and type of participation. It is important for the AMSC and COTP/FMSC to encourage industry participation in the early phases of exercise planning. If the AMSC desires industry participation, they must clearly articulate the expectations and ability of the exercise to fulfill requirements for exercising both the AMSP and participating industry plan(s). Vessels and facilities regulated by 33 C.F.R. Parts 104, 105, or 106 are required to maintain and exercise individual Vessel/Facility Security Plans (VSP/FSP).

[2] Exercises conducted to meet VSP/FSP regulatory requirements must include implementation of the specific VSP/FSP, a test of the security program, and include substantial active participation of relevant company, vessel and facility personnel. Observation of a discussion-based AMSTEP exercise by a Facility/Vessel Security Officer would not be sufficient to meet the VSP/FSP exercise requirement, but may meet a quarterly drill requirement for their facility/ship if elements of the VSP/FSP are tested in the AMSTEP exercise.

(d) Exercise Participation by Specialized Forces. Participation by specialized forces (e.g., special teams, Maritime Safety and Security Teams (MSST)) may also be appropriate depending upon exercise objectives and scenarios. Participation by these types of assets must be requested through the appropriate Coast Guard chain of command during the Multi-Year Training and Exercise Program (MTEP) process as outlined in Reference (b). However, normally the AMSTEP exercises should focus on local resources as the baseline for assessing the level of supplemental support in any given scenario.

(e) Multiple Contingency Exercises. AMSTEP exercises may be integrated with contingency or response exercises in which maritime security or Marine Transportation System (MTS) recovery is relevant. The security elements of the exercise must, at the minimum, satisfy the AMSTEP standards specified by this enclosure.

[1] A significant attribute of AMSPs is the linkage they provide to other response and recovery plans related to transportation security incidents. This recognizes that security incidents and/or terrorism events will likely cause secondary impacts (e.g., oil spills, hazardous materials releases, mass casualties) which require response actions along with the implementation of protective security measures, and recovery operations. The ability to execute these plans simultaneously and in a coordinated manner is an important concept that needs to be included in the AMSTEP exercise and preparedness program objectives. AMSCs and COTPs/FMSCs are encouraged to exercise multiple plans/contingencies in this manner. Care must be taken to

ensure that the exercises are well coordinated/integrated and that key AMSP objectives are met and avoid activities that would dilute or adversely impact the benefits of conducting the AMSTEP exercise.

[2] Multiple contingency exercises that test the AMSP and other contingencies should be coordinated between the appropriate Area and District program managers.

(f) Comprehensive Port Exercise Concept. The concept of a comprehensive port level exercise involves both the implementation of the AMSP as well as several individual vessel/facility security plans in response to a scenario. While this more holistic approach increases the complexity of the exercise effort, it also enhances the ability of port stakeholders to assess the preparedness of the relevant agencies and organizations.

(g) Use of Situational Awareness and Decision-Making Tools. Use of DHS and Coast Guard alerts, situational awareness, information sharing, and other decision-making tools is essential to ensuring that decisions are made using the best information available. The selection of tools to be used during exercises and events will rest with the senior operational commander.

(h) AMSTEP Exercise Scheduling. Numerous government and non-government organizations (including the private sector and other port stakeholders) are involved in the development and execution of Homeland Security exercise programs. AMSTEP and other exercises may be coordinated or integrated into a single, larger event if practicable to meet the objectives of both AMSTEP and other exercises more efficiently. Consideration should be given to attending applicable Training and Exercise Plan Workshops (TEPW) as outlined in Reference (b). AMSCs are encouraged to review the exercise scheduled of other government, state, tribal, territorial, or local agencies and the Contingency Preparedness System to take advantage of opportunities to participate in other exercises and to avoid conflicts with other scheduled exercises.

(i) Exercise Funding. Coast Guard funding for exercises involving AMSPs will be managed in accordance with Reference (b). Whenever possible, AMSCs should investigate and consider all sources of resources consistent with applicable rules and regulations.

(j) Exercise Support. Support for AMSTEP exercises may be available through Exercise Support Teams as discussed in Reference (b).

(k) External Affairs. COTPs/FMSCs should consult with AMSCs and with their Coast Guard District Public Affairs staff to develop strategies for

obtaining media coverage of AMSTEP exercises, while also protecting sensitive (e.g., SSI, classified) information.

(l) AMSTEP Evaluation. Evaluation criteria for an AMSTEP exercise will be generated during the development of the Evaluation Plan, and must be based on the AMSP elements being tested and associated exercise objectives.

(m) Documentation of AMSTEP Exercises.

[1] After Action Reports (AAR). The COTP/FMSC is responsible for completing the exercise AAR, following the provisions of References (b) and (c), and coordinating with the AMSC.

[2] Security Vulnerabilities. Items in AARs or Lessons-Learned that identify security vulnerabilities must be designated SSI in accordance with References (b) through (f).

(n) Relationship of Exercises to AMSP Improvements. Section 8000 of the AMSP template addresses procedures for continuous review and update of AMSPs at the port level. Lessons-Learned from AMSTEP exercises should be reflected in updates to the AMSP. Serious deficiencies in the plan or performance should be corrected within 90 days of the release of the After Action Report. Updates of critical areas of the AMSP must be submitted to the cognizant District and Area Commanders for review and approval. Critical areas requiring review and approval are defined in the AMSP Checklist developed and maintained by the Area Commanders. Recommended changes to AMS policy should be forwarded to Coast Guard Headquarters (CG-FAC) via the chain of command.

Tab A: AMSTEP Standards

AREA MARITIME SECURITY TRAINING AND EXERCISE PROGRAM (AMSTEP) STANDARDS

The table below (on pages 4-A-2 through 4-A-5) titled *Area Maritime Security (AMS) Program Standards for Exercising AMSP Elements* identifies standards for testing elements of AMSPs through AMSTEP Exercises. The comments immediately below provide an overview of the table:

- Objective: A principal objective of AMSTEP is to test AMSPs using the core AMSP elements as the basis for developing exercise objectives and scenarios.

- Linkage to National Preparedness Goal: The "Mission Area" column on the left side of the table corresponds to "Table 1: Core Capabilities by Mission Area" contained in the National Preparedness Goal. The list of Mission Areas is also contained at the end of the table on page 4-A-5.

- Regulatory Requirement: Although all AMSP elements should be covered during each four-year AMS cycle, plan elements that are specified by 33 C.F.R. § 103.505 must be included within the AMS cycle to satisfy the regulatory testing requirement.

- Frequency: The minimum frequency at which plan elements should be included in an exercise is indicated in the "Frequency" column on the right side of the table.

- Organization: Plan elements have been organized into natural groupings to encourage testing of multiple elements of the plan simultaneously where practicable.

- Consolidation: Corresponding elements located in different sections of the AMSP may be consolidated to conserve and optimize exercise planning and resources. For example, procedures for raising Maritime Security (MARSEC) levels prepared during the prevention phase and raising MARSEC levels as a security response may be exercised concurrently.

AREA MARITIME SECURITY (AMS) PROGRAM STANDARDS FOR EXERCISING AMSP ELEMENTS				
Mission Areas	**AMSP Section or Sub-Section**	**33 C.F.R. § 103 Requirement**	**Plan Element**	**Frequency**
1, 2, 4	3400 (less 3420)		Communication of AMS Information	Annual
1, 2, 4	3400	103.310(b) 103.505(l)	• Communications with Port Stakeholders	
1, 2, 4	3400	103.505(q)	• Communications with the public	
1, 2, 4	3430	103.505(b) 103.505(h)	• Communication of MARSEC Directives	
1, 2, 4	3440	103.310(b) 103.505(b) 103.505(h)	• Communication of Changes in MARSEC levels	
1, 2, 4	3420		Security Reporting Procedures	Annual
1, 2, 4	3420	103.505(r)	• Reporting suspicious activity	
1, 2, 4	3420	103.505(g)	• Reporting breaches of security	
1, 2, , 4	3500		Information Security	Annual
2, 4	3500	103.505(m)	• Sensitive Security Information	
2, 4	3500/1620	103.505(m)	• Protected Critical Infrastructure Information	
1, 2, 4	4200-4500		Maritime Security Level Procedures	Twice per cycle
2, 4	4210	103.505(o)	• Vessel at a higher security level than the facility or port it is visiting	
1, 2, 4	4300	103.505(a)	• MARSEC Level 1 operational and physical measures	
1, 2, 4	4400	103.310(b) 103.505(b)	• MARSEC Level 2 security measures	
1, 2, 4	4500	103.310(b) 103.505(b)	• MARSEC Level 3 Security measures	

AREA MARITIME SECURITY (AMS) PROGRAM STANDARDS FOR EXERCISING AMSP ELEMENTS				
Mission Areas	**AMSP Section or Sub-Section**	**33 C.F.R. § 103 Requirement**	**Plan Element**	**Frequency**
1, 2, 4	4300 4400 4500	103.505(n)	• Security measures for MTS infrastructure and activities not otherwise covered by a Vessel or Facility Security Plan, approved under 33 C.F.R. § 104-106.	Twice per cycle
1, 2, 4	4600	103.505(w)	Public Access Facility Security Measures	Once per cycle
1, 2, 4	3440 4300 4400 4500 5110	103.310(b) 103.505(a) 103.505(b)	Increase MARSEC levels	Once per cycle
1, 4	5200	103.505(g)	Preventive Measures during Security Response	Twice per cycle
1, 2, 3, 4	5210	103.505(e)	• Dangerous Substances and Devices in restricted areas	
1, 2, 3, 4	5220	103.505(f)	• Unauthorized access to designated restricted areas	
1, 2, 4,	5300		Protect Port from Vessel-Specific Security Threats	Once per cycle
1, 2, 3	5310	103.505(g)	• Procédures for Vessel Quarantaine or Isolation	
1, 2, 3	5320	103.505(e) 103.505(f) 103.505(g)	• Procedures for Security Segregation of Vessels	
3, 4	5330	103.505(i)	Procedures for Port Evacuation	Once per cycle
1, 2, 4	5400		Respond to Security Threats below the Level of a TSI	Twice per cycle
1, 2, 4	5400	103.505(g)	• General procedures	

AREA MARITIME SECURITY (AMS) PROGRAM STANDARDS FOR EXERCISING AMSP ELEMENTS				
Mission Areas	**AMSP Section or Sub-Section**	**33 C.F.R. § 103 Requirement**	**Plan Element**	**Frequency**
2, 4	5410	103.505(g) 103.505(r)	• Respond to Suspicious Activity	Twice per cycle
2, 4	5420	103.505(g)	• Respond to Breaches of Security	
2, 4	5430	103.505(p)	• Respond to Activation of a Vessel Security Alert System (SSAS) on board a Vessel within or near the Port	
2, 4	3600 5500		TSI Planning	Three times per cycle *(Use each of the three primary TSI planning scenarios at least once as a core theme of an exercise during the 4-year cycle)*
2, 4	5510	103.505(u)	• TSI Scenarios	
2, 4	3600 5520	103.505(t) 103.505(u)	• Procedures for Responding to TSI	
1-5	5530	103.505(s)	Linkages with Other Plans (to include section 5531 and/or 5532 if applicable)	Twice per cycle
1-5	5600		Transportation Security Incident Management	Twice per cycle
4, 5	5610 5630 5640	103.505(c) 103.505(u)	• Incident Command Structure and Activation	
2, 4	5620	103.505(k)	• Notification of TSIs	
3, 4, 5	5660	103.505(v)	MTS Recovery Unit *(Activation of core staff)*	Twice per cycle

4, 5	6100-6300		MTS Recovery Planning	Twice per cycle
4, 5	6100 6200 6300	103.505(v)	• MTS Recovery Framework • Recovery Roles, Authorities, Responsibilities, and Funding Streams • MTS Recovery Preparedness	
4, 5	6400-6500		MTS Recovery Process *(Implementation)*	Twice per cycle
4, 5	6400	103.505(v)	• Restoration of Commerce Following Threatened TSI • Post-Incident Recovery (Short-term)	
4, 5	6500	103.505(v)	• Post-Maritime TSI Salvage Response (Removal of Obstructions to Navigation)	

National Preparedness Goal Mission Areas

1. Prevention (e.g., Intelligence and Information Sharing, Interdiction and Disruption, Screening, Search and Detection)
2. Protection (e.g., Cybersecurity, Interdiction and Disruption, Screening, Search, and Detection, Physical Protective Measures, Risk Management for Protection Programs and Activities)
3. Mitigation (e.g., Community Resilience, Risk and Disaster Resilience Assessment, Threats and Hazard Identification)
4. Response (e.g., Critical Transportation, Infrastructure Systems, Operational Communications, Situational Assessment)
5. Recovery (e.g., Infrastructure Systems, Short-Term Economic (i.e., MTS) Recovery)

Tab B: AMS Exercise Objectives

SAMPLE AREA MARITIME SECURITY EXERCISE OBJECTIVES (FOR DISCRETIONARY USE)

1. OVERVIEW.

This Tab identifies the Major Areas of Emphasis, along with example supporting objectives that COTPs/FMSCs and Area Maritime Security Committees (AMSCs) may use when planning and executing AMSTEP exercises. The exercise objectives should be based on the high priority AMSP elements that are to be tested and other supporting needs as determined by the COTP/FMSC and AMSC.

2. MAJOR AREAS OF EMPHASIS.

a. **AWARENESS**: The COTP/FMSC and AMSC should evaluate their ability to maintain situational awareness of the port in order to balance the requirements of port security and the interests of commerce in the MTS. This evaluation should include validation of risk assessments, geographic areas of interest and jurisdictional boundaries, and resource information needed for security prevention and response planning. The evaluation should also include testing of communications of security related information among AMSP stakeholders. These objectives may be accomplished through a combination of outreach activities, and required periodic drills.

Awareness Sample Objectives.

- Demonstrate 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 and emergency situations.

- Test notification process for communicating security information, MARSEC directives, and/or changes in MARSEC levels to appropriate entities.

- Demonstrate communication of security and threat information to the Public in non-emergency and emergency settings.

- Test the expected timeframes for communicating, responding to, and tracking attainment of changes in MARSEC level.

- Verify procedures to inform vessel and/or facilities operators not covered by 33 C.F.R. Parts 104-106 of changes in MARSEC levels.

- Verify procedures for addressing situations when entities cannot, or do not, comply with their security plans when a change in MARSEC level occurs.

- Verify procedures for identification of inbound/outbound commercial vessels during a 24-hour period.

- 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-hour contact information for each FSO.

- Validate procedures for COTP/FMSC to conduct spot-checks of security measures employed by vessels and facilities within four hours of receiving reports of MARSEC Level 2 attainment, and immediately advise owners/operators of any concerns.

- Verify protective security measures (both physical and cyber) within the port established for each MARSEC level.

- Verify procedures to outline how the COTP/FMSC will conduct checks of security measures employed by vessels and facilities within one hour of receiving reports of MARSEC Level 3 attainment, and immediately advise owners/operators of any concerns.

- Test ability to properly handle and safeguard Sensitive Security Information (SSI).

b. **PREVENTION.** Test the ability of the COTP/FMSC/AMSC and port community to effectively implement security procedures, physical security measures, and Command, Control, and Communications (C3) during MARSEC Level 1/2/3 conditions. Validate risk mitigation strategies, including assessing the appropriateness and effectiveness of pre-designated preventive security measures. Validate roles, responsibilities, resources and authorities for prevention activities.

Prevention Sample Objectives.

- Test procedures used by COTPs/FMSCs to ensure that an increase in the MARSEC level is communicated to inbound vessels.

- Verify notification procedures required when a MTSA-regulated vessel and facility are operating at different MARSEC levels.

- Test procedures for assessment and approval of equivalent security measures proposed by a MTSA-regulated facility for a MARSEC Directive requirement.

- Test the COTP/FMSC review process for security procedures at all MARSEC Levels.

- Verify the security procedures identified in the AMSP for all MARSEC Levels.

- Verify authorities, roles, and responsibilities and resources to implement security procedures at all MARSEC Levels.

- Verify the adequacy of security measures in the AMSP for all MARSEC Levels.

- Verify the availability of resources to implement security measures at all MARSEC Levels.

- Verify the additional security measures required for facilities that are not regulated by 33 C.F.R. 104, 105, or 106 at all MARSEC Levels.

- Verify the adequacy of mechanisms to ensure that MTSA-regulated vessels and facilities implement security measures at all MARSEC Levels.

- Verify the adequacy of procedures identified in the AMSP for all MARSEC Levels.

- Verify the adequacy of procedures in Vessel Security Plans for vessels calling on a Public Access Facility (PAF).

- Review the list of PAFs and COTP/FMSC conditions; evaluate if designations remain appropriate.

- Verify the adequacy of security measures identified for implementation at PAFs during all MARSEC Levels.

- Test the ability of the COTP/FMSC to ensure that security measures specified for PAFs are implemented.

- Verify the adequacy of physical security measures and mitigation strategies implemented at PAFs.

c. **PROTECTION.** Test the ability of the COTP/FMSC/AMSC and port community to effectively implement enhanced security procedures, physical and other security measures, and C3 resulting from changes in MARSEC levels or receipt of threat information. Validate risk mitigation strategies, including assessing the appropriateness and effectiveness of pre-designated protective security measures. Validate roles, responsibilities, resources and authorities for security activities.

Protection Sample Objectives.

- Verify roles, responsibilities, resource availability and authorities, organizational structures coordination arrangements, and communications appropriate for protection activities.

- Verify the adequacy of physical security measures and mitigation strategies to be implemented in the port at all MARSEC Levels.

- Verify the adequacy of Information Technology/Operational Technology (IT/OT) security measures and mitigation strategies to be implemented in the port at all MARSEC Levels.

- Test procedures for and implementation and verification of increases in MARSEC levels and MARSEC level attainment.

- Verify roles, responsibilities, authorities, and available resources to implement protective measures at each MARSEC level.

- Verify procedures to respond to a report of suspicious activity within the port and the timeframes for such a response.

- Verify procedures for evacuation within the port in case of security threats or breaches of security.

- Verify pre-incident or post-incident security activities in response to threats including increases in the MARSEC levels, or to Transportation Security Incidents (TSIs).

d. **SECURITY RESPONSE.** Test the ability of the COTP/FMSC/AMSC and port community to: respond to suspicious activity, breaches of security, and Transportation Security Incidents (TSIs); organize response activities using the Incident Command System in accordance with NIMS protocols; conduct security responses, implement linkages with appropriate federal, state, tribal, territorial, and local response plans; and maintain MARSEC level operations while simultaneously conducting other response operations. Validate roles,

responsibilities, authorities, and resources for response activities.

Security Response Sample Objectives.

- Test the ability to establish a UC/IC, to include roles, responsibilities, resource availability, authorities, jurisdictions, interagency coordination, and communications appropriate for response activities.

- Test procedures for reporting of a TSI, including notifications to the National Response Center, the National Cybersecurity Communications Integration Center (for cyber incidents that do not impact physical security or environmental elements within the maritime domain), the Coast Guard chain of command, and local authorities.

- Verify procedures for implementing specific security instructions issued by the FMSC at MARSEC Level 2 or 3, in response to a TSI.

- Evaluate the ability to establish a unified command structure in response to a TSI in accordance with the AMSP including the use of NIMS and participation by appropriate agencies and stakeholders.

- Verify procedures for developing a specific incident action plan in response to a TSI, using existing IAP templates and function plans for specific AMS contingencies.

- Test procedures to respond to a report of suspicious activity or a breach of security within the port and timeframes for such a response.

- Verify adequacy of the security responses to the TSI scenarios most likely to occur within AMSC's AOR, as defined in the AMSP.

- Verify knowledge of linkages to appropriate federal, state, local, tribal and territorial response plans in response to a TSI.

- Verify and test resources required to respond to a TSI.

- Test the ability and adequacy of resources to conduct simultaneous security and other response operations (e.g., SAR, environmental response).

- Evaluate the AMSC's understanding of the goals and objectives of the National Maritime Transportation Security Plan, the National Response Framework (NRF), and the National Cyber Incident Response Plan as they apply to TSI responses.

e. **MARINE TRANSPORTATION SYSTEM RECOVERY.** Test the ability of the COTP/FMSC/AMSC and port community to stabilize the system and recover MTS functionality and resumption of trade following a TSI or the threat of a TSI. Validate the post-incident recovery of maritime critical infrastructure and key resources. Validate the process for prioritizing recovery efforts for maritime critical infrastructure and key resources. Validate roles, responsibilities, resources, authorities, and coordination arrangements for recovery activities.

MTS Recovery Sample Objectives.

- Verify roles, responsibilities, resource availability, authorities, organizational structures, coordination arrangements, and communications appropriate for MTS stabilization and recovery activities.

- Test the ability to establish an appropriate incident command or unified command structure, using NIMS protocols and participation by appropriate agencies and stakeholders.

- Test the ability of the response organization to operate within a UC/IC, to include roles, responsibilities, resource availability, authorities, jurisdictions, interagency coordination, and communications appropriate for MTS stabilization and recovery activities.

- Verify procedures and preparedness to establish and support an MTS Recovery Unit (MTSRU) within the Planning Section of an UC/IC.

- Verify procedures for determining AMS measures needed during (and in support of) MTS recovery activities.

- Verify/test linkages to other contingency plans referenced in the MTS Recovery Section of the AMSP.

- Test procedures for assessing damage to MTS infrastructure and the post-incident functional capabilities of the MTS, specifically tracking MTS stabilization and recovery status (e.g., levels of functional restoration by EEI category).

- Test procedures for determining support needed in the local area (e.g., FEMA Stafford Act mission assignments).

- Verify setting and adjustment of priorities for MTS stabilization and recovery of maritime Critical Infrastructure Key Resources (CIKR), including essential cargo flow/resumption of trade.

- Test the process for determining and prioritizing "downstream" effects on dependent and interdependent CIKR sectors.

- Test the effects of a threat of a TSI on intermodal transportation and supporting infrastructure serving a port complex.

- Test procedures for coordination and/or resumption of trade/marine commerce, and associated vessel transits within ports, waterways and access routes.

- Verify procedures to provide post-incident security for MTSA-regulated vessels.

- Verify procedures to provide post-incident security for affected MTSA-regulated facilities.

- Test/evaluate procedures to provide post-incident security for infrastructure, special events, vessels, passengers, cargo and/or cargo handling facilities with a maritime nexus within the port not regulated by 33 C.F.R. Parts 104-106, but which impacts the MTS. Verify procedures and criteria for determining the timeline for reducing specific security measures to normal levels after a security threat or incident.

TAB C: Exercise Credit Procedures

PROCEDURES FOR REQUESTING AREA MARITIME SECURITY EXERCISE CREDIT FOR OTHER EXERCISES AND REAL WORLD EVENTS

1. DISCUSSION.

a. The guidance in this Tab applies to exercises and real world operations that are not entered in the Coast Guard's Contingency Preparedness System (CPS) as an AMSTEP exercise, or as a crisis management exercise conducted by another governmental agency or from an AMSC covering a large geographical area (e.g., Regional Subcommittee).

b. Elements of other exercises and actual security operations such as MARSEC level increases, implementation of enhanced security measures, implementation of AMSP MARSEC Level 1 plan elements, National Special Security Events (NSSE), and Department of Defense (DOD) military exercises may adequately test elements of the AMSP, and would therefore be eligible for credit towards meeting AMSTEP exercise requirements. Reference (a) authorizes Coast Guard Area Commanders (as the AMSP Approving Authority) to consider, and when appropriate, authorize credit for exercises or actual operations to be used towards fulfillment of AMSTEP exercise requirements (i.e., equal to an operations-based or a discussion-based exercise as determined by the nature of the request). The circumstances of real world security operations, implementation of MARSEC Level 1 plan elements or other exercises that correspond with elements of the AMSP must be at a suitable level of effort to satisfy AMSTEP standards described in Reference (b).

c. Ultimately, the best approach to test AMSP elements is through scheduled operations-based or discussion-based exercises. However, the option of requesting exercise credit for actual security operations can be used to reduce exercise burden.

2. PROCEDURE FOR REQUESTING EXERCISE EQUIVALENCY CREDIT.

a. Coast Guard Captains of the Port (COTPs), in their role as Federal Maritime Security Coordinators (FMSC), may request equivalency credit for security or recovery exercises conducted with other government, state, tribal, territorial, or local agencies and actual operations (as defined in previous section) to be used towards fulfillment of AMSTEP exercise requirements.

b. Requests for exercise credit must be made in writing by the COTP/FMSC, and submitted through the appropriate Chain of Command to the AMSP Approving Authority.

c. The request must document the exercise scenario and objectives or real world

operation circumstances sufficiently to substantiate the request, for example:

- Link to AMSP elements involving Prevention, Protection, Mitigation, Response, and Recovery (as per the National Preparedness Goals).

- Link to AMSP elements specified by 33 C.F.R. 103.505.

d. The AMSTEP is intended, in part, to provide partners and stakeholders an opportunity to assess their capabilities to implement procedures contained in AMSPs. Other exercises or real world security operations may or may not provide an equivalent opportunity for this purpose. Therefore, the request for credit must include the written endorsement/recommendation of the AMSC Chair.

3. GUIDELINES AND CRITERIA FOR EQUIVALENCY CREDIT.

The AMSP Approving Authority may consider authorizing exercise equivalency credit if the following minimum circumstances exist:

a. The AMSP was implemented in response to actual threats or real world events, the implementation of enhanced security measures, implementation of AMSP MARSEC Level 1 plan elements or security or recovery exercises conducted with other government, state, tribal, territorial, or local agencies.

b. For credit involving real world events or actual threats where, at a minimum, a significant increase in security or recovery planning coordination and activity applicable to a Transportation Security Incident (TSI) or other type of transportation disruption was implemented.

c. For credit involving the implementation of enhanced security measures or AMSP MARSEC Level 1, where at least two plan elements listed in TAB A were implemented.

d. Members of the AMSC were involved in the response to the actual threat, real world event, implementation of enhanced security measures, and implementation of AMSP MARSEC Level 1 plan elements or security/recovery exercise conducted with other government, state or local agencies.

e. The event/exercise was consistent with AMSP program standards for testing the AMSP.

f. The effectiveness of the AMSP elements or strategies and/or tactics implemented were evaluated and are identified as standards in Tab A requiring testing.

g. The response or recovery was adequately documented and there is a favorable AMSC

recommendation to the COTP/FMSC for allowing credit.

4. DOCUMENTATION.

a. A credit request memo must provide the following information and data (normally reported in the AAR and Remedial Action Issue (RAI) and can attach to memo):

(1) The type of event and exercise for which credit is requested.

(2) Date, time, and location of the event or exercise.

(3) Description of the event or exercise.

(4) The objectives met in the event or exercise.

(5) The sections of the AMSP that was used or implemented in the event or exercise as per the previous guidelines and criteria elements.

(6) Lessons learned including an AMSC analysis of the response or recovery compared to procedures and measures included or incorporated in the AMSP.

(7) A statement verifying that the After Action Report and lessons learned were completed and associated with a COE number in the Contingency Preparedness System (CPS) IAW reference (c).

(8) The sections of the AMSP that require improvements including best practices.

(9) A timeline for AMSP improvements or documentation for immediate corrective actions implemented with approval of the FMSC.

(10) Person(s) responsible for updating the AMSP if substantive changes are to be made.

(11) Supporting Data. Enclosures should include copies of all Situation Reports (SITREPS), Incident Action Plans (IAPs), and other documentation supporting the type of event/exercise.

(12) The recommendation of the AMSC to COTP/FMSC.

b. Documentation for all requests for exercise equivalency credit must conform to applicable security classification or security designation requirements.

c. A template to assist commands in the development of a request for AMSTEP exercise credit is included in this Tab.

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

Commanding Officer
U.S. Coast Guard
[REQUESTING UNIT]

Requesting Unit Address
Staff Symbol:
Phone:
Fax:
Email:

3010
[DATE OF REQUEST]

MEMORANDUM

From: *[Requesting COTP/FMSC]*
[REQUESTING UNIT]

Reply to *[TITLE/NAME]*
Attn of: *[POC PHONE]*

To: CG (Name of Area)AREA (__-57/55)
Thru: CCGD(Name of District)(d*[XX]*)

Subj: REQUEST FOR AREA MARITIME SECURITY TRAINING AND EXERCISE PROGRAM (AMSTEP) EXERCISE CREDIT

Ref: (a) Enclosure (4) to Guidelines for the Area Maritime Security Committees and Area Maritime Security Plans Required for U.S. Ports, Navigation and Vessel Inspection Circular (NVIC) 9-02 (Series), COMDTPUB P16700.4

1. The *[NAME OF AMSC]* Area Maritime Security Committee requests AMSTEP exercise credit for the period of *[DATES]*. The *[NAME OF AMSP]* AMSP was implemented in response to *[LIST TYPE OF ACTUAL THREAT OR EVENT,* implementation of enhanced security measures, implementation of AMSP MARSEC Level 1 plan elements *OR NAME OF EXERCISE CONDUCTED WITH OTHER GOVERNMENT AGENCIES]*.

2. Appropriate members of the *[NAME OF AMSC]* AMSC were involved in response to this *[EVENT/EXERCISE]* and they determined that it has met the objectives and minimum standards for assessing the AMSP as outlined in reference (a). An evaluation of the effectiveness of the plan strategies actually implemented was conducted by *[LIST PERSON/ENTITY THAT CONDUCTED THE EVALUATION]*. It was determined that the strategies listed in the AMSP *[SATISFACTORILY/UNSATISFACTORILY]* addressed the issues, which occurred. These lessons learned are included in this request and after action report [attached].

3. This *[EVENT/EXERCISE] [PROVIDE A DESCRIPTION OF THE EVENT/EXERCISE]*. The following objectives were met: *[LIST OBJECTIVES]*. Sections *[LIST SECTIONS]* of the AMSP were used.

4. The following lessons learned were gathered during the evaluation of this *[EVENT/EXERCISE]*: *[LIST LESSONS LEARNED]*. The *[NAME OF AMSC]* AMSC conducted an analysis of the response compared to activities outlined in the AMSP. They concluded that *[PROVIDE ANALYSIS]*.

5. Sector/MSU *[UNIT NAME]* has entered an After Action Report (AAR) and lessons learned into the Coast Guard's Contingency Preparedness System (CPS) [include AAR and Remedial

Action Issues as enclosures to this memo]. It was determined that Sections *[LIST SECTIONS]* of the AMSP would require improvements.

6. Pertinent updates to the AMSP, including best practices, shall be completed within 90 days following receipt of credit approval by Commander, *[ATLANTIC/PACIFIC]* Area. *[TITLE/NAME OF PERSON]* is responsible for updating the AMSP.

#

ENCLOSURE (5) to NVIC 09-02 CHANGE 5

CYBER INCIDENT RESPONSE PLAN TEMPLATE

AREA MARITIME SECURITY PLAN (AMSP) GUIDANCE

GUIDANCE FOR DEVELOPMENT AND MAINTENANCE OF THE AMSC CYBER INCIDENT RESPONSE PLAN

1. PURPOSE. (U) The following template provides guidance to the Area Maritime Security Committee (AMSC) with the preparation and maintenance of the AMSC Cyber Incident Response Plan. This plan provides an operational framework for coordinating system stabilization of the Marine Transportation System (MTS) within a specific Captain of the Port (COTP) Zone due to a cyber incident.

2. BACKGROUND. (U) The *DHS National Cyber Incident Response Plan (*NCIRP*)* was developed according to the direction of Presidential Policy Directive 41 (PPD-41) signed on July 26, 2016. The NCIRP was promulgated in December 2016 and describes a national approach to dealing with cyber incidents; addresses the important role that the private sector, state and local governments, and multiple federal agencies play in responding to incidents and how the actions of all fit together for an integrated response. It applies to significant cyber incidents that are likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. For purposes of the maritime domain this equates to a cyber event that could cause or contribute to a Transportation Security Incident (TSI). The plan serves as the primary strategic framework for cyber TSI response.

3. DISCUSSION.

   a. (U) The DHS NCIRP illustrates a national commitment to strengthening the security and resilience of cyber technologies and infrastructure. This plan, using DHS NCIRP as a foundation, will outline the structure and content from which the COTP, in conjunction with the AMSC, can use to develop an organization specific operational response. The plan should be updated as needed to incorporate lessons-learned, to reflect opportunities and challenges that arise as technology evolves, and to ensure the plan adequately addresses a changing threat/hazard environment.

   b. (U) The NCIRP and this plan consists of several guiding principles to include:

      (1) Shared Responsibility. Shared role between entities to protect and manage cyber incidents and potential consequences.

      (2) Risk-Based Response. Determination of response actions and needed resources based on an assessment of the risks involved.

      (3) Respecting Affected Entities. Safeguard privacy, civil liberties, and sensitive private sector information when required under law.

      (4) Unity of Governmental Effort. Coast Guard coordinates joint planning for anti-terrorism efforts (to include cyber) in the port environment to enhance deterrence

and response to Transportation Security Incidents (TSIs) and maritime terrorism threats.

(5) Procedural AMSC Response. As per this NVIC, for cyber security TSIs or other marine transportation disruptions/threats, assign roles for the response and respected capabilities and link to other federal, state, local, tribal, territorial, and local plans as needed for enabling, restoration, and recovery efforts.

AMSC CYBER INCIDENT RESPONSE PLAN TEMPLATE

TABLE OF CONTENTS

ANNEX 10100, AMSC CYBER INCIDENT RESPONSE PLAN TEMPLATE

[THIS TEMPLATE PROVIDES A FRAMEWORK FOR CYBER INCIDENT RESPONSE AFTER A CYBER INCIDENT THAT RESULTS IN OR CONTRIBUTES TO A TRANSPORTATION SECURITY INCIDENT (TSI) AS DEFINED IN 33 C.F.R. 101.105]

ADAPTATION AND USE OF THIS TEMPLATE WILL BE OPTIONAL UNLESS [INSERT COTP ZONE HERE] HAS IDENTIFIED A CYBER ELEMENT AS ONE OF ITS THREE TOP TSIS SCENARIOS IN SECTION 5500 OF THE AMSP [REFERENCE (C)].

THE AMSC CYBER INCIDENT RESPONSE PLAN SUPPORTS PRESIDENTIAL POLICY DIRECTIVE (PPD-41), THE NATIONAL PREPAREDNESS SYSTEM, AND THE NATIONAL INCIDENT MANAGEMENT SYSTEM.

WHEN INCLUDED AS AN ANNEX TO AMSPS, INCLUDE PARAGRAPH MARKING FOR SECURITY DESIGNATIONS.

[TEMPLATE TEXT IS SHOWN IN **REGULAR** *FONT. SUGGESTED AND INFORMATIONAL TEMPLATE TEXT IS SHOWN IN* ***ITALICS****.]*

REFERENCES:

(a) DHS National Cyber Incident Response Plan, DEC 2016
(b) USCG CG-5P Policy Letter No. 08-16, "Reporting Suspicious Activity and Breaches of Security," 14 DEC 2016
(c) *[COTP ZONE]* Area Maritime Security Plan
(d) The Cybersecurity Information Sharing Act of 2015, 6 U.S.C. §§ 1501, Public Law 114-113
(e) FAA Reauthorization Act of 2018, 46 U.S.C. §§ 70112, Div J, Section 1805, Public Law 115-254
(f) USCG CG-FAC Policy Letter No. 02-16, "Guidance for Area Maritime Security Committee Cyber Subcommittees," 03 MAR 2016
(g) *Incorporation of local/state cyber response plans*

1000 (U) CYBER INCIDENT RESPONSE PLAN.

1100 (U) Area of Responsibility.

[(U) THE GEOGRAPHICAL AREA OF THE [INSERT COTP ZONE HERE], AS DEFINED IN 33 CODE OF FEDERAL REGULATIONS (C.F.R.) [INSERT SPECIFIC 33 C.F.R. CHAPTER 3 CITE HERE {RECOMMENDATION IS TO COPY FROM SECTION 1600 OF THE BASE AMSP}.]

1200 (U) Pre-incident Conditions/Preparedness.

[USE THIS SECTION TO LIST ANY ADVANCE PREPARATIONS NEEDED TO COORDINATE MARINE TRANSPORTATION SYSTEM (MTS) STABILIZATION DURING A RESPONSE.]

(a) (U) The purpose of this Plan is to ensure effective government and private sector security measures are being coordinated in a manner that allows all responding entities to implement plans and procedures designed to deter, detect, disrupt, respond to, and recover from a cyber security specific incident that could result in a TSI.

(b) (U) Preparedness. The following pre-incident preparations and actions will be implemented to support cyber incident response planning and activities during incident management.

[USE THIS SECTION TO LIST ANY ADVANCE PREPARATIONS NEEDED TO COORDINATE A RESPONSE. INCLUDE THE EXISTENCE AND STRUCTURE OF THE CYBER-SUBCOMMITTEE OR THE SUBCOMMITTEE THAT ADDRESSES CYBER SECURITY.]

(c) (U) The Area Maritime Security Committee (AMSC) will share information with its members and partners and facilitate assistance from capable supporting organizations to affected entities.

[ADD OTHER COMMITTEES AND STAKEHOLDERS AS APPROPRIATE.]

(1) (U) Identify communications systems and capabilities that are available to coordinate cyber incident response planning operations, to include the Coast Guard's HOMEPORT portal, video/teleconference capabilities, Homeland Security Information Network (HSIN), advisory group meetings, and other methods as appropriate.

[INCLUDE ABOVE IN THIS PLAN OR INCORPORATE BY REFERENCE AS AVAILABLE FROM SECTION 3400 AND SECTION 3600 OF THE AMSP OR OTHER PERTINENT PLANS.]

(2) (U) Identify procedural framework for prioritizing response efforts at each MARSEC Level/Condition.

[DEVELOP PROCEDURES FOR PRIORITIZATION OF THE RESPONSE, REFERENCE TAB B.]

(3) (U) Train and exercise the plan (as per the standards listed in Enclosure 4 of the NVIC 09-02 series) and periodically review to ensure framework is still relevant to evolving technical cyber challenges. [*BEST PRACTICE EXAMPLE: THE AMSC CYBER SUBCOMMITTEE WILL DEVELOP AN ANNUAL TRAINING AND EXERCISE PLAN, AND SUBMIT IT TO THE AMSC EXECUTIVE COMMITTEE DURING THE FOURTH FISCAL QUARTER FOR THE FOLLOWING FISCAL YEAR. THE PLAN SHOULD INCLUDE AT LEAST ONE EXERCISE AND ONE TRAINING EVENT FOR COMMITTEE MEMBERS AND PORT PARTNERS.]*

(4) *(U) [BEST PRACTICE EXAMPLE: THE AMSC CYBER SUBCOMMITTEE WILL REVIEW THIS PLAN AND THE ATTACHED TABS FOLLOWING EACH EXERCISE AND INCIDENT AND SUBMIT ANY CHANGE RECOMMENDATIONS TO THE AMSC EXECUTIVE COMMITTEE FOR APPROVAL.]*

(5) *(U) [BEST PRACTICE EXAMPLE: AREA MARITIME SECURITY (AMS) ASSESSMENT {SEE SECTION 3200 (A) OF THIS PLAN}. THE AMSC CYBER SUBCOMMITTEE CONDUCTS AN ANNUAL ASSESSMENT ON CYBER RISK AND ADDRESSES STRATEGIES IN ACCORDANCE WITH REFERENCE (C).]*

(6) *(U) [LIST OTHER LOCAL PREPARATIONS AS APPROPRIATE.]*

1300 (U) <u>Assumptions</u>.

[INSERT ASSUMPTIONS OF CONDITIONS OVER WHICH THE PLANNERS HAVE NO CONTROL. ALSO, INCLUDE CONDITIONS THAT, IF THEY DO NOT OCCUR AS EXPECTED, WILL INVALIDATE OR SUBSTANTIALLY ALTER THE PLAN AND NECESSITATE A CHANGE TO THE WAY THE RESPONSE WILL BE PLANNED OR CONDUCTED. UNIVERSAL ASSUMPTIONS FOR NATIONWIDE CONSISTENCY ARE LISTED BELOW.]

(a) (U) Some cyber incidents affecting the MTS may not be immediately identified as cyber related.

(b) (U) The speed at which cyber incidents can unfold is extremely unpredictable.

(c) (U) The non-regulated entities in the port are not required but are encouraged to report cyber incidents.

(d) *(U) [LIST LOCAL ASSUMPTIONS AS APPROPRIATE.]*

1400 (U) Memorandums of Agreement/Understanding.

[LIST, ATTACH OR INCORPORATE BY REFERENCE ANY MTS-RELATED MEMORANDUMS OF AGREEMENT/UNDERSTANDING PERTAINING TO A CYBER INCIDENT.]

1500 (U) Legal Considerations.

[LIST SIGNIFICANT LEGAL AUTHORITIES UPON WHICH CYBER INCIDENT RESPONSE PLANNING AND OPERATIONS ARE BASED.]

(a) (U) Reference (d) provides liability and other legal protections to private sector and certain State, Local, Tribal, and Territorial (SLTT) government organizations and establishes important conditions regarding sharing information with the Federal Government, SLTT government organizations, and the private sector.

(b) (U) This Cyber Incident Response Plan does not modify existing laws, policies, regulations or agreements regarding cyber incident response in *[INSERT COTP ZONE NAME]*.

1600 (U) Definitions.

(a) (U) General. The following definitions are general guides, and while this terminology shows up in this and similar guidance it is important to note these terms are not substitutes for definitions contained in law, regulation, or official Coast Guard policy.

(b) (U) Definitions.

(1) (U) Cyber Incident. Actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

(2) (U) Cybersecurity. The prevention of damage to, unauthorized use of, or exploitation of, and, if needed, the restoration of electronic information and communications systems and the information contained therein to ensure confidentiality, integrity, and availability; includes protection and restoration, when needed, of information networks and wire line, wireless, satellite, public safety answering points, and 911 communications systems and control systems.

(3) (U) DHS National Cyber Incident Response Plan (NCIRP). Developed to leverage the doctrine from the National Preparedness System, which articulates how the Nation responds and recovers from significant cyber incidents.

(4) (U) National Cybersecurity and Communications Integration Center (NCCIC). A 24 x 7 cyber situational awareness, incident response, and management center that is a national nexus of cyber and communications integration for the Federal Government, intelligence community, and law enforcement. Serves as a central location where a diverse set of partners involved in cybersecurity and communications protection coordinate and synchronize efforts. NCCIC's partners include other government agencies, the private sector, and international entities. Working closely with its partners, NCCIC analyzes cybersecurity and communications information, shares timely and actionable information, and coordinates response, mitigation and recovery efforts.

(5) (U) National Response Center (NRC). The NRC is the national communications center, continuously manned for handling activities related to response action in reference to maritime suspicious activities, breaches of security and TSIs. As discussed in reference (b), owners or operators are required by 33 C.F.R. 101.305 to report cyber incidents that may result in a TSI, or is by definition a TSI.

(6) (U) Significant Cyber Incident. The NCIRP uses the term to describe a cyber incident that is (or a group of related cyber incidents that together are) likely to result in demonstrable harm to the national security interests, foreign relations, or economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people. For AMSP purposes, the term is interchangeable with TSI.

(7) (U) Transportation Security Incident (TSI). A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area in accordance with 33 C.F.R. § 101.105.

(8) *(U) [ADD OTHER DEFINITIONS AS APPROPRIATE.]*

2000 (U) MISSION

2100 (U) General Roles and Responsibilities. [Each section can list additional entities and their roles pertaining to a specific COTP Zone.]

(a) (U) The *[Insert COTP ZONE name]* AMSC in conjunction with the AMSC Cyber Subcommittee *[OR OTHER AMSC SUBCOMMITTEE THAT FOCUSES ON CYBER ELEMENTS]* will*:*

(1) (U) Coordinate AMSC cyber preparedness efforts in accordance with this plan.

(2) (U) Assist the local USCG *[INSERT COTP ZONE NAME]* with the implementation of this plan as per the AMSC charter and Section 3400 of reference (c).

(3) *(U) [OTHER GENERAL ROLES/RESPONSIBILITIES AS APPLICABLE FOR LOCAL RESPONSE.]*

2200 (U) Federal Government.

(a) (U) The following summary identifies general institutional roles and responsibilities:

(1) (U) The NRC or NCCIC serves as the communications and reporting hub for cyber incidents that effect MTSA regulated facilities and vessels as per reference (b).

(2) USCG *[insert COTP ZONE name]* Command Center *[OR OTHER IDENTIFIED INTERNAL COMMAND POST]* will serve as the local communications and response hub for cyber incidents that could cause or contribute to a TSI.

(a) (U) Maintain up-to-date points of contacts to support this plan as listed on the unit's MTS Cyber Incident QRC.

(b) (U) Receive reports of MTS cyber incidents via NRC or NCCIC and conduct information sharing in accordance with this plan and *[INSERT COTP ZONE NAME]* AMSP.

(c) (U) If contacted directly by a MTS entity (MTSA regulated or non-MTSA regulated) for assistance with a cyber incident, ensure the information is passed to the appropriate organization in accordance with reference (b) and the *[INSERT COTP ZONE NAME]* AMSP.

(3) (U) Local FBI Division.

(a) (U) As per reference (a): Conducts threat response activities including investigative, forensic, analytical, and mitigation activities, interdiction of a threat actor, and providing attribution.

(b) (U) Lead federal law enforcement and national security investigative activities at the affected entity's site, link related incidents, and identify additional affected or potentially affected entities.

(4) (U) National Cyber Investigative Joint Task Force (NCIJTF). The NCIJTF is a multi-agency center hosted by the FBI and is the primary platform to coordinate the federal government's threat response to cyber incidents. *[THE LOCAL FBI DIVISION CAN SERVE AS AN INTERMEDIARY BETWEEN THE AMSC AND NCIJTF]*

(5) (U) National Cybersecurity and Communications Integration Center (NCCIC). As an operational element of the Department of Homeland Security, the NCCIC is the primary resource to coordinate the federal governments' asset response to cyber incidents. The NCCIC can support owner/operators with a wealth of technical support, including:

(a) (U) Cyber threat intelligence, alerts, and advisories.

(b) (U) Cyber security assessments.

(c) (U) Provide recommendations for improving overall network and control systems security through the National Cybersecurity Assessment and Technical Services (NCATS) which is available at no-cost to stakeholders (ncats_info@hq.dhs.gov).

(d) (U) Preliminary diagnosis to determine the extent of the compromise.

(e) (U) Provide mitigation strategies and assist asset owners and operators in restoring service.

(f) (U) In some circumstances, deploy a fly-away team to review network architecture, identify infected systems, image drives for analysis, and collect other data as needed to perform thorough follow on analysis.

(6) (U) Coast Guard Cyber Protection Team (CPT). The CPT is a deployable team of Coast Guard Cyber Command's (CGCYBER)

Network Operations & Security Center capable of conducting the mission of evaluating cybersecurity threats and vulnerabilities through a mission impact analysis to identify risks and develop mitigation and countermeasure recommendations. CPT members can serve as an effective liaison between the Captain of the Port (COTP) and the impacted entity during a cybersecurity incident, providing process or technical guidance as needed. To request CPT assistance contact the CGCYBER Battle Watch Captain (BWC) at CGCYBER-SMB-NOSC-BWC@USCG.MIL or by dialing 866-424-2478, option 4.

2300 (U) State, Local, Tribal, and Territorial Governments.

(a) (U) The following summary identifies general institutional roles and responsibilities:

(1) (U) *[INSERT STATE NAME]* Fusion Center *[*if applicable*]*.

(a) (U) Coordinate and disseminate non-sensitive/non-identifying information to government and/or critical infrastructure partners.

(b) (U) Notify federal, state, and local agencies and port partners of cyber incidents.

(c) (U) Collect and analyze cyber incident information following the incident's conclusion.

(2) (U) *[INSERT STATE/LOCAL NAME]* Law Enforcement Special Division [if applicable].

(a) (U) Assist with the criminal cyber investigations as needed within the Unified Command structure.

(b) (U) Provide as needed investigative response and triage resources.

(3) (U) *[INSERT STATE/LOCAL NAME]* Emergency Management Operations Center [if applicable].

(a) (U) Coordinate preparedness for all hazards, including cyber incidents.

(b) (U) Coordinate response to cyber security incident as needed/requested.

(c) (U) Collect, analyze, and share information with appropriate agencies/entities in regards to any affected state, local, and private sector critical infrastructure.

(4) (U) Local governments. For cyber incidents impacting the MTS in their jurisdiction, the following may apply:

(a) (U) Receive and respond to 911 call.

(b) (U) Notify appropriate agencies.

(c) (U) Participate in Unified Command.

2400 (U) Industry.

(a) (U) The following summary identifies general institutional roles and responsibilities:

(1) (U) Owner/Operator.

(a) (U) Establish cyber security efforts in accordance with the results of an internal vulnerability assessment to protect and restore critical information systems from cyber incidents in order to ensure system confidentiality, integrity, and availability as per 33 C.F.R. 104.305, 105.305, 106.305 or other applicable guidance and policies.

(b) (U) Manage the effects of the cyber incident on the organization's operations, customers, and workforce, to include complying with various legal, regulatory, or contractual obligations.

(c) (U) Report the cyber incident as required by law, regulation, or policy; or to seek assistance with threat or asset response.

3000 (U) EXECUTION

3100 (U) Concept of Operations.

(a) (U) The intent of the *[INSERT COTP ZONE NAME]* AMSC response is to minimize impacts to the MTS from a cyber incident that could cause or contribute to a TSI.

(1) (U) AMSC Intent.

(a) (U) Members and partners receive timely information to effectively respond.

(b) (U) Awareness of available assistance from the AMSC, outside agencies, organizations, and requests for assistance that are referred to the appropriate agencies.

(c) (U) The COTP/Federal Maritime Security Coordinator (FMSC) may require greater coordination over regulatory assets.

(d) *(U) [INCLUDE ANY ADDITIONAL AMSC INTENTS HERE.]*

(2) (U) Cyber Incident Scoring System/Criteria.

(a) (U) Incident scoring criteria enable an objective evaluation of an incident's severity. Their purpose is to assist with incident triage, escalation processes, and determining the prioritization of limited incident response resources and the necessary level of support for each incident. Reference (a) provides additional background.

(b) (U) Intent is to assist the affected owner/operator to assess the:

(i) (U) Severity of a given incident;

(ii) (U) Urgency required for responding to a given incident;

(iii) (U) Seniority level necessary for coordinating response efforts; and

(iv) (U) Level of investment required for response efforts.

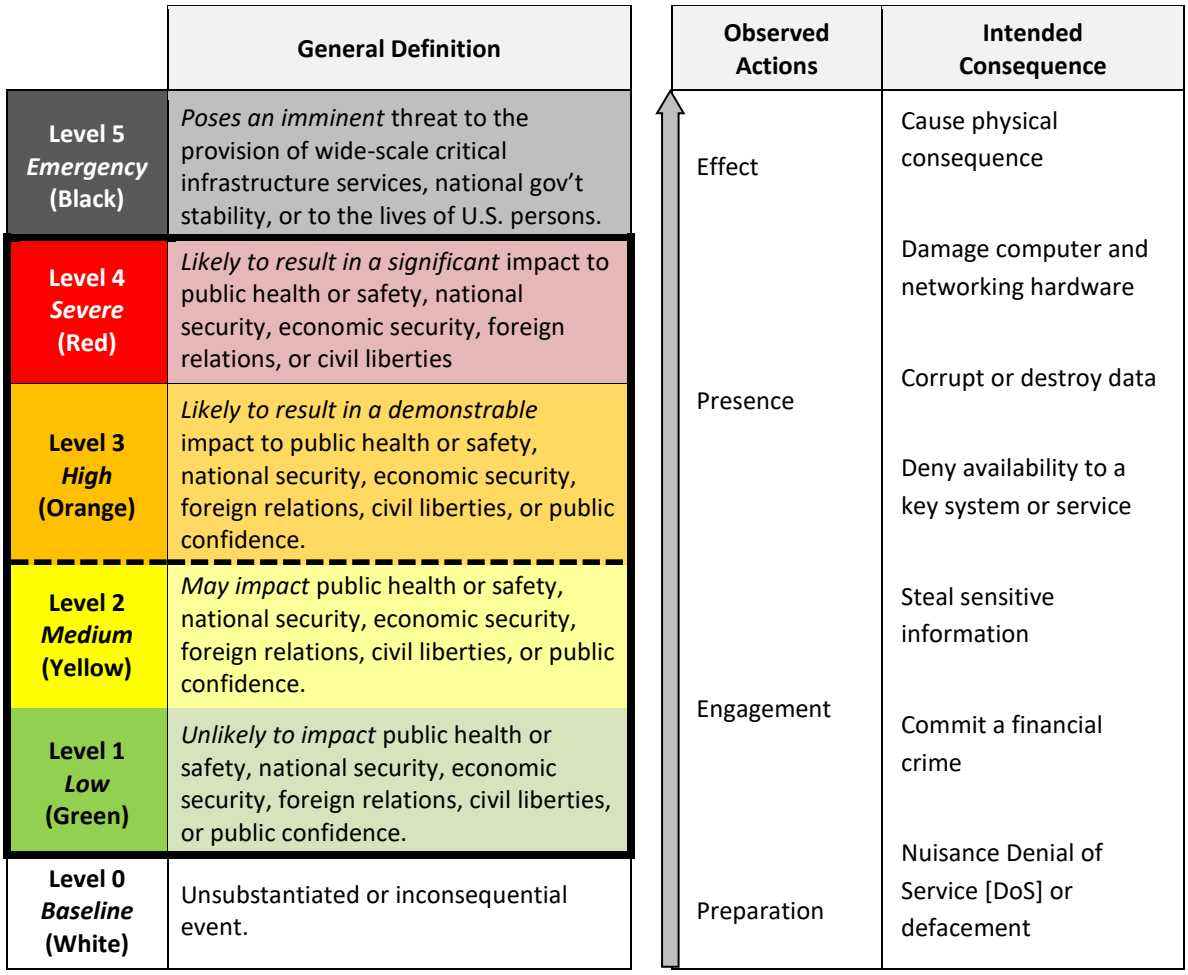


Figure 1. Elements of the Cyber Incident Severity Schema, from the *National Cyber Incident Response Plan, 2016*.

[NOTE: THE AMSC CAN ASSIST IN FACILITATING REQUESTS FOR TECHNICAL ASSISTANCE FROM INDUSTRY OWNERS AND THEIR COMPANY/FACILITY SECURITY OFFICER OR EQUIVALENT TO EVALUATE SCORING CRITERIA AS PER ANNEX C OF REFERENCE (A).]

3200 (U) Tasks.

(a) (U) Core Capabilities. Each core capability identified in the National Cyber Incident Response Plan (NCIRP) has critical tasks that are essential to achieving the desired outcome of the capability. Critical tasks inform mission objectives, which allow planners to identify resourcing and sourcing requirements prior to an incident. Using Annex F from reference (a), identify the *[INSERT COTP ZONE NAME]* AMSCs critical tasks associated with the applicable capabilities in preparing for a potential port wide cyber incident impact to the MTS *[NOTE: RECOMMEND INDIVIDUAL OWNER/OPERATORS CONDUCT IN HOUSE CAPABILITIES ASSESSMENT]*.

(1) (U) Critical Tasks

(a) (U) Critical Task #1

(b) (U) Critical Task #2 *[ADD MORE AS NEEDED]*

(b) (U) Protective Measures. Reference or add the mitigating strategies listed in section 9500 of the *[INSERT COTP ZONE NAME]* AMSP.

3300 (U) Coordinating Instructions.

(a) (U) Organization Approach to Cyber Incident Response

(1) (U) AMSC Coordination.

(a) (U*)* One role of the AMSC is to share information to increase awareness within the *[INSERT COTP ZONE NAME]* maritime community of cyber security resources for both preparation and response. The AMSC does not manage cyber incidents. Individual committee members may themselves manage the incident or serve under an incident management framework. The AMSC supports incident managers, committee members, and port partners by facilitating information sharing and requests for assistance. The AMSC acts as an information-sharing network as per Reference (e), with the USCG *[INSERT COTP ZONE OR UNIT NAME]* or other identified internal command post, which assists with ensuring significant cyber incident information is passed to the correct entity when there is a need to know.

(b) (U) The AMSC facilitates information sharing through understanding of its members and partners' information requirements and through secure and reliable means of communication. These types of information include:

(i) (U) Reports required under MTSA for regulated vessels and facilities when there is a need to know.

(ii) (U) Actionable information concerning threats of malicious cyber activity.

(iii) (U) Impacts from cyber incidents that could lead to a TSI.

(iv) (U) Technical mitigation, response, and recovery methods.

(v) (U) *[OTHER TYPES OF INFORMATION DEEMED APPLICABLE.]*

(c) (U) The AMSC facilitates requests for assistance by understanding the types of response that affected entities require and that supporting agencies can provide, and advising affected entities with their requests for help. These types of assistance include:

(i) (U) Threat response. Threat response activities include investigative, forensic, analytical, and mitigation activities, interdiction of a threat actor, and providing attribution. Threat response activities also include law enforcement and national security investigative activities at the affected entity's site, linking related incidents, and identifying additional affected or potentially affected entities.

(ii) (U) Response Activities. Response activities include furnishing technical assistance to affected entities and mitigating further consequences of a significant cyber incident.

3400 (U) Incident Reporting and Handling Requirements.

(a) (U) Incident reporting.

(1) (U) Reference (b) promulgates policy for use by MTSA regulated vessels and facilities outlining the criteria and process for suspicious activity and breach of security reporting. In accordance with 33 C.F.R. 101.305, MTSA regulated vessels and facilities shall:

(a) (U) Report suspicious activity and breaches of security for cyber incidents to the National Response Center (NRC) at 1-800-424-8802.

(b) (U) The Coast Guard allows CG regulated reporting parties to call and report a cyber incident to the National Cybersecurity and Communications Integration Center (NCCIC) in lieu of the NRC if the incident does not involve a physical and/or pollution aspect. It is imperative the reporting party inform NCCIC at the time of the call that they are a regulated CG entity that has to report the incident to satisfy reporting requirements of 33 C.F.R. 101.305. The NCCIC will forward the report electronically to the NRC, who in turn will notify the appropriate COTP. If strictly a cyber incident NCCIC may be able to provide technical assistance to the reporting party. The NCCIC can be reached at (888) 282-0870.

(c) (U) Facility and vessel operators may also make reports directly to the local COTP; however, this does not relieve an owner or operator from the requirements of 33 C.F.R. part 101.305.

(2) (U) TAB A informs port partners as to who should report, what and when to report, how to report, and to whom to report cyber incidents. The TAB is a guide and does not preempt regulated entities from complying with existing laws, policies, regulations or agreements regarding cyber incident response reporting.

(b) (U) Information handling requirements.

(1) (U) Any information related to cyber incidents is particularly sensitive and must be handled accordingly. The following classifications may apply to cyber incident information depending on the circumstances. Information will be handled in strict accordance with applicable laws, regulations, and protocols.

(a) (U) Sensitive Security Information (SSI). SSI is a specific category of information that requires protection against disclosure. The U.S. Coast Guard handles all reports of security incidents as SSI, in accordance with 49 C.F.R. part 1520, which includes requirements for proper marking and storage. The information is therefore not subject to routine public disclosure. The U.S. Coast Guard will share the information with other law enforcement agencies on a need to know basis.

(b) (U) Traffic Light Protocol (TLP). TLP is a set of designations used to ensure sensitive information is shared with the appropriate audience. It was developed by U. S. Computer Emergency Readiness Team (CERT). It employs four colors to indicate expected sharing boundaries to be applied by the recipient(s). TLP is not a “control marking” or classification scheme. TLP labels and their definitions are not intended to have any effect on the Freedom of Information Act or “sunshine” laws in any jurisdiction. The NCCIC will use TLP in its alerts and notifications to industry. Such NCCIC reporting is typically issued with identifying information redacted. If interested in receiving alerts visit www.us-cert.gov/ncas/alerts.

(c) (U) Law Enforcement Sensitive (LES). The specific definition of LES information varies from agency to agency, but it is generally defined as unclassified information of a sensitive and proprietary nature that if disclosed could cause harm to law enforcement activities by jeopardizing investigations, compromising operations,

or causing life-threatening situations for confidential informants, witnesses, or law enforcement personnel.

(d) (U) For Official Use Only (FOUO). Federal, state, and local government agencies identify some sensitive, unclassified information as FOUO. FOUO information typically identifies information of which unauthorized disclosure could adversely impact a person's privacy or welfare, the conduct of federal programs, or other programs or operations essential to the national interest. Dissemination is limited to a need-to-know basis. Release to the public or the media is prohibited.

(e) (U) Protected Critical Infrastructure Information (PCII). In rare circumstances, information owners may request DHS certify cyber incident information as PCII. PCII cannot be disclosed through a Freedom of Information Act (FOIA) request or through a request under a similar state, local, tribal, or territorial disclosure law, be disclosed in civil litigation, or be used for regulatory purposes. PCII may only be used by a federal, state, local, tribal, or territorial government employee or contractor who has taken PCII training, has homeland security duties, and has a valid need to know that particular information. PCII is specially marked and must be safeguarded, both physically and electronically, under specific procedures to avoid any improper disclosures.

(2) (U) Public Information. Public information will be communicated in accordance with reference (c).

(c) (U) Information handling requirements

(1) (U) Information Flow. The following figure depicts information flow from a cyber incident affecting a MTSA regulated vessel or facility.

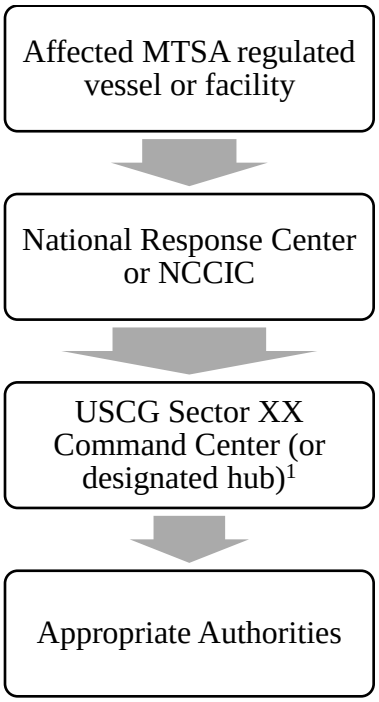


Figure 2. Information flow for cyber incidents.

[1]Coast Guard Sector should reference the most current MTS Cyber Incident QRC.

4000 (U) ADMINISTRATION AND LOGISTICS.

[WHEN USING THIS TEMPLATE IN DEVELOPING AN APPENDIX OR ANNEX TO AMSPS, YOU MAY REFER TO THE APPLICABLE SECTIONS OF THE [INSERT COTP ZONE NAME] AMSP WHERE AVAILABLE.]

4100 (U) Concept of Support

(a) (U) All organizations engaged with a cyber incident response are responsible for their own administration and logistics. Participating organizations, at their discretion, may report critical needs that exceed their organic capabilities to the IC/UC command for consideration of possible alternative support options.

5000 (U) INCIDENT MANAGEMENT.

[WHEN USING THIS TEMPLATE IN DEVELOPING AN APPENDIX OR ANNEX TO AMSPS, YOU MAY REFER TO THE APPLICABLE SECTIONS OF THE [INSERT COTP ZONE NAME] AMSP WHERE AVAILABLE.]

5100 (U) Incident Command System/Organization Relationships.

(a) (U) Include an Incident Command System Flow Chart and Resource List as per section 5520 of the AMSP for a cyber incident affecting the [*INSERT COTP ZONE NAME*].

5200 (U) Incident Command Post and Headquarters.

[SUMMARIZE: INCLUDE TAB IF SECTION APPLICABLE TO INCIDENT/MAY REFERENCE SECTION 5600 OF THE LOCAL AMSP.]

5300 (U) Succession to Incident Command.

[SUMMARIZE: INCLUDE TAB AS APPROPRIATE.]

5400 (U) Incident Command, Control, and Communications.

(a) (U) Requests for Assistance and Information (RFAs and RFIs). Any RFAs or RFIs received by the AMSC will be referred to the most appropriate agency for processing.

(b) (U) Information Requirements. The following are organizations that may need to know information regarding cyber incidents. *[NOTE: MAY ADD OTHER ENTITIES NOT LISTED IF APPLICABLE TO YOUR SPECIFIC COTP ZONE]*.

(1) (U) Industry owner/operator *[THE FOLLOWING IS SUGGESTED]*.

(a) (U) Cyber threat intelligence, alerts, and advisories.

(b) (U) Technical assistance for incident mitigation, response, and recovery.

(2) (U) USCG Sector Command Center [if applicable]. A cyber incident that could cause or contribute to a TSI subsequently affecting the safety or security of the *[INSERT COTP ZONE NAME]*.

(3) (U) Local FBI Division. Cybercrime, including computer intrusions or attacks, fraud, intellectual property theft, identity theft, theft of trade

secrets, criminal hacking, terrorist activity, espionage, sabotage, or other foreign intelligence activity.

(4) (U) NCCIC. Suspected or confirmed cyber incidents, including when the affected entity may be interested in government assistance in removing the adversary, restoring operations, and recommending ways to improve security.

(5) (U) State Level Law Enforcement, Fusion Center, etc. for the *[INSERT COTP ZONE NAME]* Marine Transportation System.

(6) (U) *[APPLICABLE STATE]* Department of Emergency Management. Physical impacts as a result of a cyber incident, or if it could impact public safety, health, property, the environment, or economy of *[STATE AFFILIATED WITH THE APPLICABLE COTP ZONE]*. They should be notified immediately. *[INSERT APPLICABLE STATES EMERGENCY OPERATION CENTER (EOC) 24-HOUR WATCH CENTER NUMBER]*.

(7) (U) Local Emergency Managers. Physical impacts as a result of a cyber incident, or if it could impact public safety, health, property, the environment, or economy of their jurisdiction.

(8) (U) Critical Infrastructure Sector Partners.

(a) (U) Cascading effects that could impact their operations, safety, or security.

(b) (U) Threat and asset response information.

TABS

Tab A: AMSP Cyber Incident Reporting Matrix
Tab B: MARSEC Levels and Cybersecurity Conditions

TAB A: AMSP Cyber Incident Reporting Matrix

[INSERT COTP ZONE NAME] AMSP Cyber Incident Reporting Matrix
TAB A to Annex XXXXX, Cyber Incident Response Plan, *[INSERT COTP ZONE NAME]* Area Maritime Security Plan

The purpose of this Tab is to provide port stakeholders with guidance on cyber incident reporting. The goal is to inform partners who should report, what and when to report, how to report, and to whom to report cyber incidents [existing laws, policies, regulations or agreements regarding cyber incident response reporting should be noted in remarks]. Unless otherwise indicated, the telephone numbers listed do not accept text messaging. *[NOTE: THE MATRIX CAN BE EXPANDED TO OTHER KNOWN RESOURCES]*.

Who is reporting	What to report	Report to whom	How to report	Remarks
MTSA regulated vessels and facilities	Cyber suspicious activity and/or breaches of security that impact physical security or cause pollution	National Response Center (NRC)	1-800-424-8802	CG-5P Policy Letter No. 08-16, "Reporting Suspicious Activity and Breaches of Security," 14 DEC 2016 outlines the criteria and process for suspicious activity and breach of security reporting.
MTSA regulated vessels and facilities	Cyber suspicious activity and/or breaches of security that **DO NOT** impact physical security or cause pollution	National Cybersecurity and Communications Integration Center (NCCIC) - OR - National Response Center (NRC)	1-888-282-0870 or NCCIC@hq.dhs.gov - OR - 1-800-424-8802	For cyber incidents that **DO NOT** impact physical security or cause pollution, the Coast Guard highly encourages industry to contact NCCIC as the NCCIC may be able to provide technical assistance. It is imperative that the reporting party inform the NCCIC that they are a Coast Guard regulated entity in order to satisfy the reporting requirements of 33 C.F.R. part 101.305. Regulated entities can also contact the NRC directly to report cyber incidents that **DO NOT** impact physical security or cause pollution

Who is reporting	What to report	Report to whom	How to report	Remarks
Non-regulated MTS entity	1. A significant loss of data, system availability, or control of systems; 2. A large number of victims; 3. Unauthorized access or malicious software present on critical information systems; 4. Impacts to critical infrastructure or core government functions; or 5. Impacts on national security, economic security, or public health and safety.	FBI NRC NCCIC	http://www.ic3.gov/ 1-800-424-8802 (888) 282-0870 or NCCIC@hq.dhs.gov	The IC3 provides the public with a mechanism to submit information to the FBI concerning suspected Internet-facilitated criminal activity. Programs such as the American Waterways Watch promotes reporting suspicious activity to the NRC. The NCCIC serves as a central location where a diverse set of partners involved in cyber security and communications protection coordinate and synchronize their efforts.

TAB B: MARSEC Levels and Cybersecurity Conditions

[INSERT COTP ZONE NAME] MARSEC LEVELS AND CYBERSECURITY CONDITIONS
TAB B to Annex XXX, Cyber Incident Response Plan, *[INSERT COTP ZONE NAME]* Area Maritime Security Plan.

CONDITION	PORT	REGULATED FACILITIES	EXTERNAL AUTHORITIES
1 – sustained operations	• *Threat awareness brief* • *Refresher – suspicious activity and security breach procedures*	• *Threat awareness brief* • *Refresher – suspicious activity and security breach procedures*	• *Threat awareness brief* • *Broadcast POCs and maintain comm. channels*
2 – elevated threat	• *Threat awareness telcon* • *Check IDs for all remote access* • *Terminate external media use* • *Remove email attachments* • *Physical security audit of TWIC use* • *Web reputation filtering* • *Prevent mobile phone connections to systems* • *Review privileged access*	• *Threat awareness telcon* • *Check IDs for all remote access* • *Terminate external media use* • *Remove email attachments* • *Physical security audit of TWIC use* • *Prevent mobile phone connections to systems* • *IT-OT monitoring* • *Safety system surveillance* • *Review privileged access*	• *Threat awareness telcon* • *Terminate external media use* • *Outside intel search (dark web)*
3 – imminent threat/after incident	• *Implement segmentation plan* • *Remote access terminated* • *Email limits* • *Web browsing restrictions* • *IT-OT monitoring* • *Physical Inspection of TWICs* • *Restrict privileged access*	• *Implement segmentation plan* • *Remote access terminated* • *Email limits* • *Continuous IT-OT monitoring* • *Safety system security continuous monitoring* • *Web browsing restrictions* • *Physical Inspection of TWICs* • *Restrict privileged access*	• *Email limits* • *Outside threat intelligence/ surveillance*

[NOTE: THE TABLE CONTAINS SUGGESTED MEASURES; THE AMS ASSESSMENT IN SECTION 9500 OF THE AMSP MAY IDENTIFY DIFFERENT AND/OR ADDITIONAL MEASURES].

ENCLOSURE (6) TO NVIC 9-02 CHANGE 5

SALVAGE RESPONSE PLAN TEMPLATE

GUIDANCE FOR DEVELOPMENT AND MAINTENANCE OF THE SALVAGE RESPONSE PLAN

1. PURPOSE.

   a. (U) The Salvage Response Plan (SRP) is an element of the AMSP that coordinates post-maritime TSI salvage to reopen the port as required by the Security and Accountability For Every Port Act (SAFE Port Act) of 2006. This enclosure provides guidance to the Captain of the Port (COTP) on the preparation and maintenance of the SRP. The objective of the SRP is to ensure that navigable waterways are cleared of wrecks, obstructions, and similar impediments to maritime transportation in order to support the reestablishment of basic U.S. Marine Transportation System (MTS) functionality and flow of maritime commerce after a TSI. The SRP content is designed to be compatible with all forms of transportation disruptions, consistent with the guidance contained within AMSPs to deter and mitigate the effects of a TSI. The SRP should be used to guide planning in those cases in which optimization of salvage resources across multiple salvage needs is appropriate.

   b. (U) The SRP helps coordinate the application of salvage response where necessary during the short-term recovery phase after a TSI *or other transportation disruption* to ensure that waterways are cleared sufficiently to restore the flow of commerce through the MTS quickly in accordance with the objectives contained in the National Response Framework (NRF), DHS Strategy to Enhance Supply Chain Security, and AMSPs. The SRP is also used to coordinate TSI-related salvage response with salvage activities conducted in support of Area Contingency Plans. The SRP assists with the implementation of an orderly transition to the long-term recovery phase of salvage response as part of the process of restoring full functionality to navigable waterways.

2. BACKGROUND.

   a. (U) To achieve the plan's intent of restoring the resumption of commerce in the MTS, the Incident Command/Unified Command (IC/UC) must ensure planning and operations are aligned with the appropriate policy and funding mechanisms. Marine salvage may encompass the formal definition of salvage (i.e., rescuing something of value from peril) as well as wreck, obstruction, and debris removal. Each activity may have different authorities, funding sources, and levels of federal agency involvement. The principal pathways for salvage authority and funding are summarized in the subparagraphs below and in Tabs B, C, D, and F.

      (1) (U) Salvage is typically conducted at the local level on a case-by-case basis, and is normally the responsibility of vessel owners or operators, underwriters, or the parties responsible for other obstructions to navigation.

      (2) (U) Salvage is a required element within Area Contingency Plans (ACP). Salvage conducted under the auspices of the Oil Pollution Act of 1990 (OPA 90),

addresses the threat of pollution and does not necessarily result in removal of the obstruction once the pollution threat has been resolved. Specific salvage-related activities may vary between ACPs. Further information on Federal-On-Scene-Coordinator's (FOSC) job responsibilities can be found in Coast Guard Marine Environmental Response and Preparedness Manual, COMDTINST M16000.14 (series).

(3) (U) When there is a non-pollution event in which a vessel or other obstruction is creating a hazard to navigation within federally defined navigable waters, the U.S. Army Corps of Engineers (USACE) serves as the Lead Federal Agency for ensuring either removal of the obstruction from (or immediately adjacent to) the federal channel by the owner, operator, or lessee, or by effecting removal using hired labor forces or a contractor. In the latter case, USACE then seeks reimbursement from the identified owner, operator, or lessee for justified and documented removal expenditures. The Coast Guard and USACE cooperate in the removal of hazards to navigation in accordance with the provisions of Memorandum of Agreement between the Department of the Army and U.S. Coast Guard (signed in October 2005).

(4) (U) The NRF uses a construct of Emergency Support Functions (ESFs) to provide pathways for coordinating Federal Emergency Management Agency (FEMA) Mission Assignments (MAs) for nationally declared disasters that fall under the provisions of the Stafford Act (such as debris removal following a hurricane-making landfall). FEMA MAs involving salvage support are coordinated through ESF 1, ESF 3, and ESF 10.

(a) (U) The scope of authority and funding found in the Stafford Act does not extend to all potential salvage needs. Funding authorized by the Stafford Act is only accessible when there has been a Presidential Disaster Declaration.

(b) (U) The events associated with Hurricanes Katrina and Rita in 2005 demonstrated that preparations and coordination of salvage response activities were not fully developed for large-scale incidents. Subsequently, pre-scripted FEMA MAs related to salvage were developed and included in ESF 1, ESF 3, and ESF 10.

(5) (U) Unusual incidents have resulted in the use of alternative authorities and funding to support salvage operations, including the use of highway funds, special authorizations and appropriations by Congress (e.g., special appropriation for salvage and other recovery activities following the Interstate 35 Highway Bridge collapse over the Mississippi River). In unusual situations, COTPs/FMSCs should seek program and legal guidance from Coast Guard Headquarters via the chain of command.

(6) (U) The National Disaster Recovery Framework (NDRF) provides guidance for long-term recovery support to states, tribes, territories, and local jurisdictions adversely impacted by disasters. It provides a flexible structure that enables disaster recovery managers to operate in a unified and collaborative manner. It also focuses on how to restore, redevelop and revitalize the health, social, economic, natural and environmental fabric of the community, and building a more resilient nation through the use of Recovery Support Functions (RSFs).

b. (U) The SAFE Port Act of 2006 requires that each AMSP include a SRP.

3. DISCUSSION.

a. (U) The SRP provides a coordination and procedural framework for access to existing marine salvage authorities and resources. It identifies and relies on existing authorities and funding mechanisms of federal agencies and stakeholders with a marine salvage or marine services nexus. The plan also supports the unity of effort when marine salvage response is needed for resumption of trade, and to assist in restoring basic functional capability of the MTS.

(1) (U) The SRP identifies marine salvage equipment and resources that are normally located within the COTP/FMSC Zone, which are capable of being used to restore basic operational trade capacity of the MTS. The plan also addresses national salvage capabilities.

(2) (U) The SRP identifies the role of the AMSC in providing support for pre-incident preparedness and post-incident prioritization and planning of salvage activities.

b. (U) Concept of Salvage Response. The SRP includes the COTP/FMSC, AMSC and AMS process, beginning with preparedness planning up to the point at which incident-specific planning and operations are initiated to address physical impediments to navigation in the waterway.

(1) (U) Upon establishment of an IC/UC, the SRP becomes a supporting plan for salvage response and recovery managed by the IC/UC's Planning Section, supported by the Marine Transportation System Recovery Unite (MTSRU) as appropriate, and by a salvage response/marine services management team, if established. It will be used to provide coordination links to marine salvage resources.

(2) (U) All salvage response and marine services operations will be conducted by individual organizations consistent with their jurisdiction, authorities, funding sources, and capabilities, and through the IC/UC when implemented.

(3) (U) Salvage and marine services issues beyond the scope of the SRP will be referred to the IC/UC for consideration, as appropriate.

c. (U) Incident (TSI).

(1) (U) Incident. A maritime disruption caused by a TSI and resulting in a physical obstruction to the navigable waterways within the waterway.

d. (U) Incident Impact.

(2) (U) Commercial navigation within a waterway is significantly or totally obstructed, or is threatened by effects or potential effects of other obstructions in navigable waters (e.g., unstable debris field, obstructions causing adverse alterations of water flow or level, etc.).

(a) (U) Localized intermodal, labor, supply chain, and economic effects will build relative to the severity of the transportation disruption.

(b) (U) Secondary intermodal, supply chain and economic effects will vary, but will progressively increase toward levels of regional or national significance, depending on the overall circumstances of the incident.

e. (U) SRP Objectives.

(1) (U) Provide a coordinated salvage response framework to ensure that waterways are cleared to support the resumption of the flow of commerce through the MTS as efficiently and quickly as possible following a TSI or other transportation disruption.

(2) (U) Identify locally available salvage equipment capable of supporting the restoration of operational trade capacity within the MTS.

(3) (U) Supporting objectives include, but are not limited to:

(a) (U) Establish a framework for salvage response that is compatible with salvage coordination for other forms of transportation disruptions.

(b) (U) Identify available salvage response authorities, funding, and resources that may be necessary to resolve a transportation disruption as a consequence of a TSI.

(c) (U) Identify local, regional, and national salvage industry resources.

SALVAGE RESPONSE PLAN TEMPLATE FOR TRANSPORTATION SECURITY INCIDENTS

The template beginning on the next page is provided for use at the discretion of COTPs/FMSCs to assist in preparation of the Salvage Response Plan required by the Security and Accountability for Every Port Act (SAFE Port Act) of 2006. The template provides a recommended Area Maritime Security standard framework for coordinating salvage response in support of recovery of the U.S. Marine Transportation System (MTS) and resumption of commerce following a Transportation Security Incident (TSI). The template design presumes salvage response activities will be planned using a common coordination framework that is applicable across all forms of transportation disruptions (including TSIs). The focus of this plan is marine salvage and similar marine services needed to reopen navigable waterways to maritime commerce during the short-term recovery phase of incident management. "Cut and paste" text is shown in regular font. Suggested and informational template text is shown in italics.

This guidance incorporates the requirements set forth by the SAFE Port Act. It does not create new policy or change existing salvage response policy nor is it a substitute for experience and familiarity with the wide range of laws, policies, and funding mechanisms applicable to various situations. Note that outside the scope of this plan, the Coast Guard and other federal agencies have roles and responsibilities that pertain to obstructions to navigation, wrecks, debris, marking, removal, vessel casualty and pollution response activities. These responsibilities still apply within the context of a TSI.

This template is intended to promote consistency nationwide for salvage response to a transportation disruption. It also provides a framework for the COTP/FMSC, and the AMS Committees to address local salvage needs and issues.

The SRP should be considered a supporting plan for the MTS recovery planning process established during a Unified Command response to an incident. The plan should be used to identify salvage resources and post incident procedures when conducting salvage operations following a maritime transportation disruption.

Maritime salvage, wreck, and debris removal present complex and challenging operational, policy, legal, and funding issues. Each of these activities requires time and effort to address successfully. It is neither possible nor practical to develop contingency plans for the entire range of possible situations, so awareness of general principles helps the COTP/FMSC prepare for a range of events. In these situations, operational objectives include, but are not limited to safety of life and property, protection of the environment, removal and mitigation of hazards to navigation, and the functionality of the MTS.

(U) ANNEX *[Enter Annex Number Here]*, SECTOR *(Enter Sector Name here)* AREA MARITIME SECURITY PLAN

TABLE OF CONTENTS

SECTOR (*Enter Sector Name here*) SALVAGE RESPONSE PLAN

REFERENCES.

(a) Assessment of the U.S. Marine Transportation System: A Report to Congress, U.S. Department of Transportation, September 1999
(b) Security and Accountability for Every Port Act of 2006 (SAFE Port Act), Public Law 109-347
(c) Navigation and Navigable Waters, Maritime Security: Area Maritime Security, 33 C.F.R. § 103.505
(d) COTP Zone *(enter COTP Zone Name here)* Area Maritime Security Plan (AMSP)
(e) National Response Framework, June 2016
(f) Strategy to Enhance International Supply Chain Security, Department of Homeland Security (DHS), July 2007
(g) Area Contingency Plan for *(Enter plan name here)*
(h) Marine Transportation System Recovery Planning and Operations, COMDTINST 16000.28 (series)
(i) U.S. Coast Guard Incident Management Handbook (IMH), COMDTPUB P3120.17(series)
(j) Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. § 5121 et. seq., as amended
(k) Abandoned Vessels, COMDTINST M16465.43 (series)
(l) Navigation and Navigable Waters, Department of the Army, Corps of Engineers, Removal of Wrecks and Other Obstructions, 33 C.F.R. Part 245
(m) Navigation and Navigable Waters, Marking of Structures, Sunken Vessels and Other Obstructions, 33 C.F.R. Part 64
(n) Navigation and Navigable Waters, Jurisdiction, 33 C.F.R. § 2.36
(o) Interagency Agreement (IAA) between the United States Navy and the United States Coast Guard for Cooperation in Oil Spill Clean-up Operations and Salvage Operations dated 15 SEP 1980
(p) Memorandum of Agreement (MOA) between the Department of the Army and U.S. Coast Guard, October 1985

SITUATION.

(U) This plan provides a framework for planning and coordinating the post-Transportation Security Incident (TSI) salvage response activities needed to facilitate the recovery of the Marine Transportation System (MTS). As described by Reference (a), and in accordance with References (b) and (c), this plan supports the clearing of port waterways to enable the resumption of maritime commerce in the Captain of the Port (COTP) *[INSERT COTP ZONE HERE]*. These references do not create new authorities or funding sources, and this plan was developed within the constraints of existing laws and policies.

(a) (U) Pursuant to References (b) and (c), this plan identifies and relies on existing authorities, procedures, policies, funding mechanisms, and sources of technical expertise and salvage resources for incident management activities and operations needed to coordinate resumption of maritime commerce following a TSI or threat of a TSI during the short-term recovery phase of incident management. This plan serves as an Annex to the COTP Zone *[INSERT COTP ZONE HERE]* Area Maritime Security Plan, Reference (d).

(b) (U) This plan aligns with and supports Reference (e) and Emergency Support Function (ESF) 1 (Transportation), ESF 3 (Public Works and Engineering), and ESF 10 (Oil and Hazardous Materials Response) with regard to salvage response activities.

(c) (U) This plan serves concurrently as a salvage response framework in support of Reference (f) and it incorporates relevant information from Reference (g) for response to oil spills or hazardous materials releases resulting from a TSI.

(d) (U) This plan anticipates the establishment of a Unified Command (UC) under the National Incident Management System (NIMS) protocols, and the use of a common salvage response coordination framework for all forms of transportation disruptions. This plan may be adapted and used for other transportation disruptions, consistent with the overarching responsibilities of the AMSP, to deter and mitigate the effects of a TSI.

(e) (U) This plan incorporates guidance concerning coordination between the AMSC and other advisory bodies (e.g., Area Committee for response to oil spills and hazardous materials releases affecting the marine environment) regarding salvage preparedness, response priorities, and other post-incident aspects of response to inform development of the UC's Incident Action Plan (IAP).

1000 (U) SALVAGE RESPONSE PLAN (SRP).

(U) This SRP provides a framework for salvage response planning, coordination and support during the short-term recovery phase of incident management following a TSI. The SRP applies to vessels, wrecks, obstructions, and marine debris that are a physical impediment to the port navigation system within the waterway and are thereby impeding the flow of maritime commerce.

1100 (U) Area of Responsibility.

(a) (U) The geographical area of responsibility of the [insert COTP Zone here] Captain of the Port Zone, as defined in 33 Code of Federal Regulations (C.F.R.) [insert specific 33 C.F.R. Chapter 3 Cite here]

[Consider adding graphic showing area of responsibility or refer to AMSP, as appropriate.]

1200 (U) Pre-Incident Conditions/Preparedness.

(a) (U) Preparedness. The following pre-incident preparations and actions will be implemented to support salvage response planning and activities during incident management.

[Use this section to list any advance preparations needed to coordinate Marine Transportation System (MTS) salvage and refer to corresponding appendices in the plan.]

(1) (U) Identify coordinating procedures for obtaining salvage subject matter expertise and information. Coordinate salvage Subject Matter Expert (SME), information, and staffing support needs with existing bodies including Area Committees, Harbor Safety Committees, Port Readiness Committees (PRC), and AMSCs.

[PROVIDE OPPORTUNITY FOR ORGANIZATIONS REPRESENTED ON THE AMSC, AC, AND OTHER MARITIME ADVISORY GROUPS AND STAKEHOLDERS TO PROVIDE ADVISORY SERVICE IN SUPPORT OF THE MARINE TRANSPORTATION SYSTEM RECOVERY UNIT (MTSRU) AND UNIFIED COMMAND (UC). ALSO CONSIDER MEANS, SUCH AS AN AMSC SUBCOMMITTEE OR PORT COORDINATION COMMITTEE, TO FACILITATE BROAD ACCESS TO AND ANALYSIS OF TRANSPORTATION DISRUPTION INFORMATION ABOUT INCIDENT EFFECTS ON CRITICAL INFRASTRUCTURE KEY RESOURCES (CIKR) AND CARGO FLOW. A JOINT AMSC/ACP SALVAGE RESPONSE SUBCOMMITTEE IS SUGGESTED TO FACILITATE SALVAGE PREPAREDNESS. PERSONNEL DESIGNATED IN ADVANCE TO SERVE IN AN MTSRU SHOULD BECOME GENERALLY FAMILIAR WITH WRECK, OBSTRUCTION, SALVAGE RESPONSE AND MARINE DEBRIS REMOVAL

AND DISPOSITION RULES, REGULATIONS, POLICIES, AND PROCEDURES, AND MUST BE PREPARED TO ASSIST WITH THE INTEGRATION OF SALVAGE RESPONSE PLANNING AND COORDINATION INTO THE INCIDENT MANAGEMENT PROCESS.]

(2) (U) The AMSC will coordinate supporting relationships with other relevant committees.

[ADD OTHER COMMITTEES AND STAKEHOLDERS AS APPROPRIATE. SECTORS WITH PORT COORDINATION TEAMS OR OTHER ADVISORY BODIES MAY REFERENCE THEM HERE.]

(3) (U) Establish location of salvage response "planning functions" for incident management. The salvage response planning functions may be assigned to a Marine Transportation System Recovery Unit (MTSRU) established per References (d), (f), (h) and (i) or, if a MTSRU is not implemented, placed within the Planning Section within a Unified Command structure as appropriate.

(4) (U) Develop and populate salvage-specific Essential Elements of Information (EEI) in order to provide baseline salvage response information needed to initiate salvage planning during incident management. At a minimum, the EEI shall include the salvage capability information required by Reference (b). The EEI should identify infrastructure at potential choke points for maritime traffic (e.g., bridges, pipeline crossings), their owners and operators, and associated contact information. They should also support EEI requirements of Reference (h).

[THE COTP/FMSC SHOULD PROVIDE OPPORTUNITY FOR ORGANIZATIONS REPRESENTED ON THE AMSC, AC, AND OTHER MARITIME ADVISORY GROUPS AND STAKEHOLDERS TO ASSIST WITH DEVELOPMENT, VALIDATING, AND UPDATING OF EEIS AS SOON AS POSSIBLE FOLLOWING A TRANSPORTATION DISRUPTION. RELEVANT EEIS MAY BE INCORPORATED BY REFERENCE, FOR EXAMPLE, BY LINKING TO AMSPS.]

(5) (U) Identify communications systems and capabilities that are available to coordinate salvage response planning operations, to include the Coast Guard's Homeport portal, video/teleconference capabilities, advisory group meetings, and other methods as appropriate.

[INCLUDE ABOVE IN THIS PLAN OR INCORPORATE BY REFERENCE AS AVAILABLE FROM SECTION 3400 OF THE AMSP, ACP AND OTHER PERTINENT PLANS.]

(6) (U) Identify procedural framework for prioritizing salvage, wreck, and debris removal in consultation with existing advisory bodies including Area Committees, AMSCs, PRCs, and Harbor Safety Committees.

[DEVELOP PROCEDURES FOR PRIORITIZATION OF SALVAGE RESPONSE FOR WRECKS, OBSTRUCTIONS, AND MARINE DEBRIS REMOVAL ACTIONS ACCORDING TO THEIR IMPORTANCE IN RESUMING MARITIME COMMERCE, TAKING INTO CONSIDERATION THE CONTINUITY OF THE PORT NAVIGATION SYSTEM, PORT FUNCTIONS, AND DOWNSTREAM/INTERMODAL EFFECTS. SUGGEST INCLUDING THIS INFORMATION IN AN ADDITIONAL TAB TO FACILITATE REVISIONS.]

(7) (U) Describe procedures for coordinating salvage response at all MARSEC Levels.

[INSERT PROCEDURES FOR COORDINATING SALVAGE RESPONSE AT ALL MARSEC LEVELS.]

(b) (U) [List other local preparations as appropriate.]

2000 (U) ROLES AND RESPONSIBILITIES.

2100 (U) General Roles and Responsibilities.

(a) (U) Roles and responsibilities for salvage response will depend upon the circumstances of the incident.

(b) (U) Primary Responsibility.

(1) (U) If the USACE and the Coast Guard jointly determine that a sunken or grounded vessel or wreck is a hazard to navigation, it must be removed as expeditiously as possible by the Responsible Party.

(2) (U) Normally, primary responsibility for taking or arranging action to resolve an obstruction or other impediment to navigation is the identified Responsible Party of a sunken or grounded vessel or wreck; or, the Responsible Party of other obstructions in the waterway such as structures, train cars, and vehicles. Where a discharge of oil, hazardous substance release, or threat thereof is involved, primary responsibility belongs to the Responsible Party as defined by the Oil Pollution Act of 1990.

2200 (U) Federal Government.

(U) The following summary identifies general institutional roles and responsibilities. More detailed information about Federal agency roles and responsibilities is provided in Tab B.

(a) (U) U.S. Coast Guard (USCG). The Coast Guard works closely with the U.S. Army Corps of Engineers (USACE) to ensure a coordinated approach to maintaining safety and the functionality of the port navigation system in U.S. ports and waterways. The Coast Guard serves as the federal government's lead agency for responding to threatened or actual pollution incidents in the coastal zone. The Coast Guard is one of two primary agencies for ESF 10 (Oil & Hazardous Materials Response), which includes mission-specific salvage response. The Coast Guard, upon the request of FEMA, may provide management and contract administration for certain MAs under the authority and funding in accordance with Reference (j). The COTP, as FMSC, is responsible for maintaining and implementing this SRP. Immediately upon discovery of an obstructing vessel or object, the Coast Guard has responsibilities for marking and notification as required by References (k), (l), (m) and (n). Coast Guard authority for vessel removal/destruction when no Responsible Party can be identified is described in COMDTINST 16465.5 (series), and COMDTINST M16465.43 (series).

(b) (U) U.S. Army Corps of Engineers (USACE). The USACE serves as the Federal Government's lead agency for maintaining the navigability of federal channels in domestic ports and waterways. The USACE arranges for and conducts hydrographic surveys, assessments of navigation conditions, and dredging. The USACE also has authority that may be applicable for removing wrecks from federal navigable channels, and more limited authority to address obstructions that pose hazards to navigation as discussed in References (l), (m), and (n). The USACE is one of two primary agencies for ESF 3 (Public Works & Engineering), and may provide engineering management and contract administration, at the request of the FEMA, for salvage-related MAs under authority and funding discussed in Reference (j).

(c) (U) U.S. Navy Director of Ocean Engineering, Supervisor of Salvage and Diving (SUPSALV). SUPSALV is the Department of Defense's principal source of salvage expertise. Upon request, SUPSALV may provide federal-to-federal support for salvage response. SUPSALV and the Coast Guard cooperate in oil spill clean-up and salvage operations in accordance with the provisions of Reference (o). SUPSALV can provide expertise and conduct/support specialized salvage/wreck removal operations. SUPSALV is able to draw quickly upon the extensive resources of the commercial salvage industry through its standing salvage support contracts. Additionally, SUPSALV maintains an extensive inventory of government owned assets that are pre-positioned for immediate deployment. SUPSALV can also access the Navy's hydrographic survey assets/capabilities, and can provide in-office technical support. However, funds must be provided to access SUPSALV or their capabilities.

(d) (U) National Oceanic and Atmospheric Administration (NOAA). An agency of the Department of Commerce, NOAA provides aerial and hydrographic survey support and expertise. NOAA also administers the Abandoned Vessel Program (AVP). The main objective of this program is to investigate problems posed by abandoned and derelict vessels in U.S. waters. The program maintains various information resources.

(e) (U) Environmental Protection Agency (EPA). The EPA serves as the coordinator and is one of two primary agencies for ESF 10 (Oil & Hazardous Materials Response).

(f) (U) Federal Emergency Management Agency (FEMA). FEMA is the federal lead for Mission Assignments (MAs) under Reference (i) authorities and funding. FEMA is one of three primary agencies for ESF 4 (Firefighting), one of two primary agencies for ESF 5 (Information and Planning), one of two for ESF 6 (Mass Care, Emergency Assistance, Temporary Housing, and Human Services), one of two primary agencies for ESF 7 (Logistics), and one of two primary agencies for ESF 9 (Search and Rescue). FEMA also serves as the coordinator and primary agency for Infrastructure Systems

Recovery Support Function (RSF) under the National Disaster Recovery Framework.

(g) (U) U.S. Department of Transportation (DOT). DOT serves as coordinator and primary agency for ESF 1 (Transportation).

(h) (U) National Transportation Safety Board (NTSB). The NTSB has authority and responsibility for investigation of major transportation incidents and may engage in preservation of evidence and safety investigation in conjunction with salvage operations that have not resulted from an act of terrorism.

(i) (U) Federal Bureau of Investigation (FBI). The FBI has law enforcement investigation responsibility for acts of terrorism and may engage in preservation of evidence and law enforcement investigation in conjunction with salvage operations that are in response to acts of terrorism.

2300 (U) State, Local, Tribal, and Territorial Governments.

(a) (U) State, local, tribal, and territorial governments have an important role in determining priorities and developing a rational approach to coordinating efforts to accomplish rapid marine survey, salvage, and wreck/debris removal in (or adjacent to) their jurisdictions.

(b) (U) State, local, tribal, and territorial government agencies have certain responsibilities for removal of obstructions and debris that are outside of defined federal navigable waters and do not create hazards to navigation.

(c) (U) Some states have established abandoned and derelict vessel programs for their waters to address removal of abandoned vessels that do not pose a risk that would trigger removal actions by federal agencies.

2400 (U) Industry.

(a) (U) National Salvage Capabilities.

(1) (U) American Salvage Association. Refer to www.americansalvage.org for details.

(b) (U) Local and Regional Salvage Capabilities.

[LIST OR INCLUDE AN APPENDIX IDENTIFYING LOCAL AND REGIONAL SALVAGE RESOURCES, POINTS OF CONTACT, AND CALL-UP NUMBERS.]

(c) (U) Vessel and Cargo Owners/Operators and Insurers.

(1) (U) For vessels and cargos, the owners/operators (and those that underwrite their property) retain the primary responsibility for obtaining salvage assistance when needed. Under References (l) and (m), the Responsible Party retains responsibility for marking and removal of their vessel and or cargo even if it has no remaining value. In addition, some tank vessels are required by 33 C.F.R. § 155.4030 to include/ identify salvage and marine firefighting capabilities within their respective Vessel Response Plans (VRPs). COTPs must give the Responsible Party reasonable opportunity to comply with appropriate legal requirements while protecting the value of their property.

(2) (U) The COTP must balance the ability of the Responsible Party (RP) to take appropriate action in a timely fashion. Delay in salvage or inappropriate initial action may worsen the situation, increasing impact on the marine transportation system, the environment, and/or overall cost. The COTP should not hesitate, if in doubt, to seek advice from the organizations listed in Tab B.

3000 (U) ASSUMPTIONS.

[INSERT ASSUMPTIONS OF CONDITIONS OVER WHICH THE PLANNERS HAVE NO CONTROL. ALSO, INCLUDE CONDITIONS THAT, IF THEY DO NOT OCCUR AS EXPECTED, WILL INVALIDATE OR SUBSTANTIALLY ALTER THE PLAN AND NECESSITATE A CHANGE TO THE WAY MTS RECOVERY WILL BE PLANNED OR CONDUCTED. UNIVERSAL ASSUMPTIONS FOR NATIONWIDE CONSISTENCY ARE LISTED BELOW.]

(a) (U) Reconstitution.

(1) (U) Functional capabilities and resources sufficient to support salvage response will be sufficiently restored before salvage response operations commence.

(b) (U) Salvage during Environmental Response.

(1) (U) Salvage, when conducted in conjunction with oil spills or hazardous substance releases will be initiated during the response phase under ACPs to prevent or mitigate environmental consequences.

(c) (U) Initiation of Salvage Response.

(2) (U) Deployment of salvage response resources to assist in reopening waterways to commerce will occur as soon as possible following an incident.

(d) (U) Local Assumptions.

[ADD LOCAL ASSUMPTIONS, AS APPROPRIATE.]

4000 (U) LEGAL CONSIDERATIONS.

[LIST SIGNIFICANT LEGAL AUTHORITIES UPON WHICH SALVAGE RESPONSE PLANNING AND OPERATIONS ARE BASED. LIST ANY APPLICABLE MEMORANDUMS OF AGREEMENT AND MEMORANDUMS OF UNDERSTANDING.]

(a) (U) This SRP does not in any way modify existing laws, policies, regulations or agreements regarding salvage, wreck and debris removal. Nothing in this SRP alters the rights of Responsible Parties from recovering their property expeditiously.

(b) (U) This SRP does not provide authority to contract for or conduct salvage operations nor does it provide a coordination and procedural framework for access to salvage resources, consistent with existing authorities, policy and funding.

(c) (U) This SRP identifies and relies on existing salvage authorities and funding mechanisms of Federal agencies and stakeholders with a salvage nexus for salvage response tactical planning and operations.

(d) (U) Tab B includes a listing of relevant Memorandums of Agreement (MOA) and Memorandums of Understanding (MOU).

(e) (U) Tab C lists principal federal authorities that pertain to salvage response. Tab D describes the funding considerations related to salvage response.

5000 (U) DEFINITIONS.

(U) Definitions used in this plan are included as Tab A. The definitions are general guides, and are not substitutes for definitions contained in law, regulation, or official Coast Guard policy.

6000 (U) EXECUTION.

6100 (U) Concept of Operations.

(a) (U) Incident Commander's Intent.

(1) (U) To support short-term MTS recovery by implementing a flexible framework to plan and coordinate employment of marine salvage response capabilities (within existing authorities, policy and funding constraints), to clear the navigable waterways sufficiently for resumption of maritime commerce.

(2) (U) Initiate salvage response assessments, planning, and coordination with pertinent stakeholders and salvage response providers, as soon as possible following an incident.

(3) (U) Determine appropriate uses of authorities, funding, and resources to conduct salvage response to reopen channels and waterways.

(4) (U) Identify salvage needs for MTS infrastructure, which are beyond the scope of this SRP, and provide input for development of FEMA MAs or other long-term recovery support through ESF 1, ESF 3 and/or ESF 10, as appropriate.

(5) (U) Support marine salvage operations through the IC/UC structure.

(b) (U) Concept of Salvage Response Planning and Operations.

(1) (U) The procedures in this SRP cover salvage preparedness planning up to the point at which incident-specific salvage response planning and operations are initiated. The plan also provides information on salvage resources that could be employed in responses.

(2) (U) Initial environmental response, MTS recovery actions, and identification of prospective salvage response needs will be undertaken by stakeholders using their existing operations protocols and contingency plans (e.g., existing Vessel Response Plans). Salvage issues identified will be referred to the COTP, who will communicate them as necessary to the IC/UC.

(3) (U) Upon establishment of an IC/UC, the SRP becomes a supporting plan to the Incident Action Plan (IAP) and informs salvage response planning by the MTSRU, and salvage subject matter experts during

incident management. Activities of the MTSRU will be guided by the MTS Recovery Plan for the *[INSERT COTP ZONE HERE]*.

(4) (U) Salvage issues beyond the scope of the SRP will be addressed by the appropriate ESF(s) through the IC/UC for consideration.

(5) (U) Feedback about implementation of salvage response measures and resulting effects on performance and functionality of the port navigation system will be considered in forming MTS recovery and salvage response recommendations.

6200 (U) Deployment.

(a) (U) All salvage response operations will be conducted by individual organizations consistent with their jurisdiction, authorities, capabilities, and funding availability.

(b) (U) Salvage equipment and resources based within the COTP Zone, which are capable of being used to restore the MTS may not be available. Likewise, national and/or regional salvage capabilities identified in this plan may not be available.

[IDENTIFY LOCAL SALVAGE RESOURCES AND CAPABILITIES IN TAB H. INCORPORATE SALVAGE EQUIPMENT CONTAINED IN THE AREA CONTINGENCY PLAN.]

6300 (U) Employment.

(a) (U) Salvage Operations. A salvage response team may be needed to execute salvage operations during an incident. Members assigned to the salvage response team would be responsible for developing an incident-specific salvage response plan for assigned salvage work. Therefore, salvage operations will be included as an element of the Incident Action Plan (IAP). This SRP is a supporting plan to those incident-specific response efforts.

(b) (U) Safety. A site safety plan must be developed and operations conducted in accordance with the plan under the supervision of a qualified safety officer with expertise in vessel construction, marine salvage, or commercial diving.

(c) (U) Demobilization. Salvage response resources will be released as soon as possible. For planning purposes, once clearing of appropriate navigable waterways enables the resumption of the flow of maritime commerce, salvage response activities will transition from short-term recovery to long-term recovery. The MTSRU will assist with the salvage-related transition.

As part of its demobilization report to the IC/UC, the MTSRU will prepare a list of unresolved salvage response and marine debris issues.

6400 (U) Tasks.

(a) (U) During the incident response phase, the identification of measures needed to set the stage for salvage response, as a supporting activity of MTS recovery, should be initiated. Development of salvage and MTS recovery-specific tasks should be done as part of the IAP planning process in accordance with NIMS ICS protocols.

[BRIEFLY DESCRIBE, INCLUDE AS AN APPENDIX, OR INCORPORATE BY REFERENCE, THE INFORMATION NEEDED TO IDENTIFY SALVAGE RESPONSE NEEDS AND THE COORDINATION AND DISSEMINATION OF INFORMATION. CONSIDER THE FOLLOWING LISTED ITEMS IN SCOPING AN INITIAL SALVAGE RESPONSE PLANNING WORK LIST.]

(1) (U) *[INSERT MEASURES NEEDED TO SET THE STAGE FOR SALVAGE RESPONSE OPERATIONS (E.G., BASIC SERVICES TO SUPPORT SALVAGE PERSONNEL, LOGISTICS, SAFETY, FORCE PROTECTION, SECURITY FOR SALVAGE RESOURCES.]*

(2) (U) *[INSERT RESPONSIBILITIES FOR PROVIDING AND OBTAINING INFORMATION DURING FIRST-LOOK DAMAGE AND IMPACT ASSESSMENTS.]*

(3) (U) *[INSERT DESCRIPTION OF BASIC INFORMATION NEEDED TO SUPPORT SALVAGE RESPONSE PLANNING INCLUDING WRECKS, OBSTRUCTIONS TO NAVIGATION, AND MARINE DEBRIS THAT ARE PREVENTING OR INTERFERING WITH THE FLOW OF MARITIME COMMERCE IN THE PORT NAVIGATION SYSTEM.]*

(4) (U) *[INSERT PROCEDURES FOR IDENTIFYING POSSIBLE OR PROBABLE IMPACTS FROM INITIAL ASSESSMENTS FOR MORE THOROUGH INVESTIGATION DURING SALVAGE RESPONSE PLANNING.]*

(5) (U) *[INSERT PROCEDURES FOR COORDINATION AND DISSEMINATION OF SALVAGE RESPONSE INFORMATION.]*

(6) (U) *[INSERT PROCEDURES TO INITIATE IDENTIFICATION OF RESPONSIBLE PARTIES FOR WRECKS AND OBSTRUCTIONS TO NAVIGATION.]*

(b) (U) Determine needs, arrange for, and coordinate provision of salvage response using this plan for COTP Zone _____ *[INSERT REFERENCE]* and ACP _____ *[INSERT REFERENCE]* salvage provisions, as appropriate.

(1) (U) Assess the scope of the salvage response needed, including aerial surveys to assist in identifying salvage issues and hydrographic survey of critical waterways/channels. Tab E provides guidance to assess salvage response needs.

(2) (U) Use the SRP as a coordination and procedural plan to support identification and application of existing salvage authorities and funding mechanisms when salvage response becomes necessary. Tab F provides general SRP considerations. Tab G provides SRP-related acronyms.

(3) (U) Use the ACP to guide salvage operations conducted during oil and hazardous substance environmental response activities.

(4) (U) Identify Responsible Parties (RPs) to determine their intentions for developing and executing a removal/salvage plan.

(5) (U) Assess and recommend priorities for salvage response needed to reopen the navigable waterways.

(6) (U) Coordinate with the Infrastructure Liaison Officer (ILO) at the Joint Field Office (JFO) (if established) for recovery support, including identification of recovery issues under Stafford Act disaster declarations.

(7) (U) Coordinate with the USACE in accordance with Reference (p) for removal of hazards to navigation by the Responsible Party when ownership of the hazard cannot be determined, or if removal of the hazard by the Responsible Party cannot be accomplished in a timely manner.

(8) (U) Coordinate with ESF 1, ESF 3, and ESF 10, coordinating primary and supporting agencies through the JFO (when established) to arrange for salvage response services.

(9) (U) Consistent with Reference (m), identify and coordinate the marking of obstructions and hazards to navigation by the Responsible Party, or if they fail to act in a timely manner, the Coast Guard and USACE.

(10) (U) Coordinate the establishment of an IC/UC salvage response function with subject matter expertise to conduct site-specific assessments of obstructions to navigation and salvage needs and to develop and implement salvage plans to address the obstruction(s) to navigation.

(11) (U) Identify available public and commercial salvage assets when the Responsible Party cannot be identified or respond in a timely manner.

(12) (U) Monitor impact of salvage recommendations on MTS Recovery.

(13) (U) Document salvage response activities and operations.

7000 (U) ADMINISTRATION AND LOGISTICS.

[*Refer to the applicable Sections of the AMSP for incident management as appropriate. Supplement here as appropriate*.]

7100 (U) Concept of Support.

(a) (U) All providers are responsible for determining and establishing the adequacy and appropriateness of the authorities and funding under which they will provide salvage response.

(b) (U) All government and private industry organizations participating in salvage response are responsible for coordinating their own administration and logistics until unified coordination of administration and logistics is implemented by the IC/UC.

(c) (U) Participating organizations should report essential needs that exceed their organic capabilities to the IC/UC.

8000 (U) INCIDENT COMMAND, CONTROL, AND COMMUNICATIONS.

[WHEN USING THIS TEMPLATE IN DEVELOPING THE SRP ANNEX TO THE AMSP, REFER TO THE APPLICABLE SECTIONS OF THE AMSP FOR INCIDENT MANAGEMENT. IF PROCEDURES DIFFER FROM THOSE IN THE AMSP, LIST EXCEPTIONS BELOW]

8100 (U) Command Structure Relationships/Organizational Relationships.

[SUMMARIZE. INCLUDE APPENDIX AS APPROPRIATE.]

8200 (U) Incident Command Posts (ICPs) and Headquarters.

[SUMMARIZE. INCLUDE APPENDIX AS APPROPRIATE.]

8300 (U) Succession to Incident Commander.

[IDENTIFY PRIMARY, DEPUTY AND ALTERNATES AS APPROPRIATE.]

8400 (U) Incident Command, Control, and Communications.

[SUMMARIZE. INCLUDE APPENDIX AS APPROPRIATE.]

TABS

Tab A: Salvage Response Plan Definitions
Tab B: Federal Agency Salvage-related Roles and Responsibilities
Tab C: Federal Authorities Related to Salvage
Tab D: Funding Considerations Relating to Salvage Response
Tab E: Guidance to Assess Salvage Response Needs
Tab F: Notional Salvage Response Framework
Tab G: Glossary of Acronyms
Tab H: Local Marine Salvage Capabilities

Tab A: Definitions

SALVAGE RESPONSE PLAN DEFINITIONS

1. (U) General. The definitions included in this Tab are general guides, and are not substitutes for definitions contained in law, regulation, or official Coast Guard policy. As informally used, the term "salvage" encompasses a broad range of topics including salvage, wreck, obstruction and debris removal, and aspects of spill response.

2. (U) Definitions.

   a. (U) Hazard to Navigation: An obstruction, usually sunken, that presents sufficient danger to navigation so as to require expeditious, affirmative action such as marking, removal, or redefinition of a designated waterway to provide for navigation safety (33 C.F.R. Part 245).

   b. (U) Debris: The definition of debris (e.g., construction and demolition debris, general debris, marine debris, wet debris) may vary between jurisdictions and legal authorities. For the purposes of this plan, the applicable definition must be determined by the facts pertaining to each incident. When dealing with debris issues, the COTP and any other involved party must ensure they have the authority and funding to act in a specific instance. The following general definitions are included as information resources to support incident-specific determinations.

      (1) (U) Construction and Demolition Debris. Includes damaged components of buildings and structures such as lumber/wood, gypsum wallboard, glass, metal, roofing material, tile, carpeting and floor coverings, window coverings, pipe, concrete, fully cured asphalt, equipment, furnishing, and fixtures. (Public Assistance: Debris Management Guide, FEMA-325, June 2014.)

      (2) (U) Debris (Stafford Act). Items and materials broken, destroyed, or displaced by a natural or man-made (federally declared) disaster. Examples of debris include, but are not limited to, trees, construction and demolition material, and personal property. Materials classified as debris under the Stafford Act will vary by incident. (*Public Assistance: Debris Management Guide, FEMA-325, June 2014).*

      (3) (U) Marine Debris/Floatable Debris. No definition that can be universally applied. However, marine debris is typically characterized as trash consisting of floatable materials and saturated floatable materials that have become suspended or have sunk to the bottom. Marine debris may potentially include (1) floatable materials/floatable debris including trash (see subparagraph 2.b.(5) below), and (2) derelicts, which is lost, abandoned, or discarded property (e.g., abandoned sunken vessels without salvage value, lost or abandoned fishing gear, abandoned submerged vehicles or equipment).

(4) (U) Post-Disaster Waterway/Marine Debris: Includes, but is not limited to, all manner of vegetation, building material, recreational and commercial vessels, and all manner of other items that threaten the environmental and navigation safety of the navigable waters. (*U.S. Navy Salvage Report Hurricanes Katrina and Rita, January 2007*).

(5) (U) Floatable Materials. The Beaches Environmental Assessment and Coastal Health (BEACH) Act (Public Law 106-284) defines floatable materials to mean any foreign matter that may float or remain suspended in the water column and includes plastic, aluminum cans, wood products, bottles, and paper products.

c. (U) Marine Salvage. Service/assistance that is rendered to a vessel and/or her cargo to save the vessel or cargo in whole, or in part, from impending marine or maritime peril, or in recovery such property from actual maritime peril or loss, with contribution to the success by the service that was rendered by the salvor. Marine peril typically increases with time.

d. (U) Obstruction. Anything that restricts, endangers, or interferes with navigation as described in Reference (l). Obstructions can be authorized man-made structures such as bridges, pier heads, offshore towers, or unexpected interferences, which must be assessed to determine their effect on navigation.

e. (U) Area of Responsibility (see 33 C.F.R. Part 3). Federally constructed and/or maintained navigable waterways and anchorages located within the COTP/FMSC Zone and may include the transportation and/or utility structures above or below the water surface that cross or are adjacent to such channels and anchorages. Also included in the meaning of the port navigation system are the services aiding vessel navigation on the waterway such as pilotage, tug/towing services, navigation aids, harbormaster services, vessel traffic services, and police or fire services on the waterway.

f. (U) Responsible Party. Under the Oil Pollution Act of 1990, the term “Responsible Party” refers to the persons owning, operating, or chartering a vessel by demise; the owner or operator of a facility from which oil is discharged; owners and operators of pipelines; the licensees of Deepwater ports; and the persons leasing, permittee of, or holder of a right to use or easement for an area in which an offshore facility is located. The Responsible Party is liable for the costs associated with the containment or cleanup of the spill and any damages resulting from the spill. The first priority of the EPA and Coast Guard is to ensure that responsible parties pay to clean up their own oil releases. However, when the responsible party is unknown or refuses to pay, funds from the Oil Spill Liability Trust Fund can be used to cover removal costs or damages resulting from discharges of oil or threat of a discharge of oil, subject to the rules and procedures that apply.

g. (U) Salvage Award. The reward or compensation allowed by maritime law for service rendered in saving maritime property, at risk or in distress, by those under no legal obligation to render it, which results in benefit to the property, if eventually saved.

h. (U) Towage/Towing Service. Towing service that is motivated for convenience, not safety, in the absence of peril. Rescue towing or other salvage towing service that is conducted in conjunction with marine salvage is not considered towage or towage service.

i. (U) Transportation Disruption. Any significant delay, interruption, or stoppage in the flow of trade caused by natural disaster, heightened threat level, an act of terrorism, or any Transportation Security Incident (SAFE Port Act of 2006, Public Law 109-347, Section 2).

j. (U) Transportation Security Incident. A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area (33 C.F.R. § 101.105).

k. (U) Wreck. A sunken or stranded ship, or any part thereof, or any object that is lost at sea from a ship that is stranded, sunken or adrift, or any of the above that may reasonably be expected to sink or strand where activity to assist the ship or property is not underway.

l. (U) *[ADD OTHER DEFINITIONS AS APPROPRIATE.]*

Tab B: Roles and Responsibilities

FEDERAL AGENCY SALVAGE-RELATED ROLES AND RESPONSIBILITIES

1. (U) General. This Tab provides additional detail about major federal organizations participating in salvage-related activities.

2. (U) United States Coast Guard.

   a. (U) National Strike Force (NSF).

      (1) (U) The NSF may be able to assist the Sector Commander/Captain of the Port (COTP) in the below listed areas. Current NSF doctrine and policy should be consulted for available support and equipment:

         - Perform site characterization, damage assessment, take samples and mitigate release.
         - Develop safety plan for salvage operations.
         - Review commercial dive plans and monitor commercial dive operations.
         - Develop/review salvage plans.
         - Conduct vessel damage assessments.
         - Develop transfer plan, including termination plans for use in final product removal.
         - Perform basic damage control.
         - Monitor/conduct dewatering, de-ballasting, and lightering operations.
         - Assist in development/review of dewatering, de-ballasting, and lightering plans.

      (2) (U) NSF Equipment.

         - Salvage Assessment Kit. Designed for determining fluid levels of watertight compartments. The kit may also help distinguish separate fluid levels within a tank or vessel such as water in petroleum products.

- Enhanced Viscous Oil Pumping System. Designed to be incorporated into, and enhance an existing offloading pumping system. It is designed to be used when the oil characteristics to be pumped create higher frictional hose resistance than either the pump or the hose system can handle in the form of discharge pressure. Innovative manifold design enables pumping system to be used as a standard pump, cold water injected pump for viscous oils or hot water injected pump for extremely viscous products up to 200 centistokes.

- Large Pumping System. The large pumping system is designed for lightering oil tankers and cargo vessels. The pumps incorporated in the ready load (submersible and non-submersible), are capable of pumping a wide range of petroleum products, mild acids, corrosives, and water. The pumping system is pre-staged on a trailer and palletized into four segments, ready for rapid deployment by aircraft or tractor-trailer.

(3) (U) National Strike Force (NSF) assistance. Coast Guard Sector Commander/COTPs should call the Coast Guard Strike Team in their AOR or the National Strike Force Coordination Center (NSFCC) directly.

b. (U) Marine Safety Center (MSC).

(1) (U) The MSC is an engineering technical office located in Washington, D.C. The MSC works directly with the marine industry, Coast Guard Headquarters staffs, and Coast Guard field units in the evaluation and approval of commercial vessel designs, development of safety standards and policies, and oversight of delegated third parties in support of the Coast Guard's marine safety and environmental protection programs.

(2) (U) The MSC created the Salvage Engineering Response Team (SERT) in 1990 to support Coast Guard efforts with several major marine casualties. Team membership is a voluntary collateral duty for a small number of staff engineers. SERT members are naval architects trained to conduct technical analyses in the areas of vessel stability and structural integrity. The SERT can assist with marine casualties involving vessel groundings, collisions, fires, and similar emergencies. For example, the SERT's salvage engineers can provide force-to-free estimates in cases of commercial vessel groundings, review damage stability and/or structural calculations submitted by a commercial salvage company, and assist the COTP with the review of a salvage plan.

(3) Additional Information. Visit the Marine Safety Center page on the HOMEPORT website, or call (202) 475-3401. To contact the SERT, fill out a Rapid Salvage Survey form found on the MSC's HOMEPORT web site. Email the completed form to the SERT at SERT.Duty@uscg.mil, and follow-up with a phone call to the SERT Duty Officer at (202) 327-3985 (cell).

3. (U) U.S. Army Corps of Engineers (USACE).

a. (U) The USACE works with the COTP on a routine basis. The USACE has District offices that are assigned to all major ports and Federal channel projects. The following are USACE Points of Contacts (POCs):

- USACE District Emergency Operations Center: _____
- USACE District Commander: _____
- Operations Division Chief: _____
- Chief of Navigation: _____
- Local Project Operator: _____

b. (U) Each District office will have capabilities in place as required for their specific mission. Each District can provide the information about the following capabilities:

- Surveys
- Emergency dredging
- Contracts for vessel and obstruction removal
- Spill kits

c. (U) Navigation Charts. The USACE publishes paper navigation charts and Inland Electronic Navigation Charts (INEC) that contain information about structure and utility crossings of navigable waterways. This information may be useful in itemizing pertinent information about these structures and utilities in relation to prospective salvage operations.

d. (U) Funding. For large-scale disasters, natural or man-made, some of the funding for USACE activities including salvage response and debris removal operations is typically provided through supplemental appropriations.

e. (U) For contact and other information about USACE, visit:

- www.usace.army.mil/
- www.englink.usace.army.mil

4. (U) U.S. Navy Director of Ocean Engineering, Supervisor of Salvage and Diving (SUPSALV or NAVSEA OOC).

   a. (U) SUPSALV's mission is to provide technical, operational, and emergency support to the Navy, DoD, and other Federal agencies, in the ocean engineering disciplines of marine salvage, pollution abatement, diving, diving system certification, and underwater ship husbandry. SUPSALV regularly works with the Coast Guard SERT Team to assist with Program of Ship Salvage Engineering (POSSE) consultations and operational support.

   b. (U) SUPSALV is the U.S. Government national resource for salvage and oil spill response in part from operations in support of events such as the Exxon Valdez clean up and the F/V Ehime Maru recovery. SUPSALV is also the Navy Technical Authority for Salvage and Diving, Diving Systems Safety Certification, and Underwater Ship Husbandry.

   c. (U) SUPSALV is a lean organization, leveraging response through contractor support and using commercial assets through standing, open, and competitively bid salvage contracts and while providing efficient on-site project management capabilities. SUPSALV maintains the Emergency Ship Salvage Material (ESSM) System, which is a managed network of facilities and emergency response stockpiles pre-positioned to support and augment capabilities in the areas of salvage, diving, pollution response, and underwater ship husbandry. Various customers include the Navy fleet, NAVSEA Program Executive Officers (PEO), NAVAIR, SPAWAR, DoD, USCG, NTSB, NASA, NOAA, and the FBI, among others. SUPSALV is listed as a support agency within the National Response Framework under ESF 3 and 10.

   d. (U) Additional Information: For additional information, including SUPSALV points of contact, capabilities and equipment, visit www.supsalv.org. The SUPSALV main telephone line is (202) 781-1731.

5. (U) National Oceanographic and Atmospheric Administration (NOAA)

   a. (U) Office of Coast Survey

      (1) (U) Navigation Response Teams (NRT)

         (a) (U) In any given year, a variety of man-made and natural events affect U.S. waterways, ports and harbors. These changes require rapid investigation to keep maritime vessel traffic navigating safely for the nation's economic welfare.

         (b) (U) NOAA's NRTs are mobile emergency response teams equipped and trained to survey ports and near-shore waterways immediately following incidents such as a maritime accident, or a major storm that causes the sea

bottom or submerged obstructions to shift. NRTs have the ability to be transported by trailer over land from one location to another for quick response and have become a crucial part of reopening ports and shipping lanes after a hurricane.

(c) (U) Examples of NRT Responses:

- NRTs from across the country responded to the catastrophic impact caused by Hurricanes Katrina and Rita. Within a matter of days, shipping channels were able to be reopened with confidence that all obstructions had been identified and located due in part to NRT work.

- In 2004, Athos-I Tanker grounded and spilled oil in Delaware Bay. An NRT was called in to assist in the investigation and search for obstructions.

- An NRT surveyed to clear the waterway after the South Padre Island Bridge in Texas was struck by a tow in 2001, causing large quantities of debris to fall into the channel.

- NRTs have responded to clear affected ports after many hurricanes including Hurricanes George, Frances, and Ivan.

(d) (U) When not responding to emergencies, the NRTs check the accuracy of nautical charts and help address priority needs of mariners. Up-to-date nautical products reduce risk in transits and increase economic benefits to ports and the commercial vessel traffic that transport billions of dollars of goods and energy products into and out of the country. NRT surveys allow pilots to transit areas in varying weather and sea conditions with confidence that the charted positions of features critical to safe navigation are highly accurate.

(e) (U) In order to locate hazardous submerged obstructions, NRTs are equipped with state of the art hydrographic equipment. Every team has side scan sonar to provide photograph-like imagery of the entire seafloor and half the teams have multi-beam sonar to generate a three dimensional view of what lies below the surface.

(f) (U) NRT Resources. NOAA maintains six teams – two each on the East/West Coasts, one on the Gulf Coast and one in the Great Lakes.

(2) (U) <u>Navigation Managers</u>.

(a) (U) The Office of Coast Survey's representatives in the field, help decide its future activities. They serve as ambassadors to the maritime community.

Maintaining a distributed presence for its customers, Coast Surveys Navigation Managers help identify the challenges facing marine transportation in general, directly supporting the NOAA strategic goal to "promote safe navigation." These agents assist the Coast Survey in overseeing the National Oceanic and Atmospheric Administration's nautical chart data collection and information programs, helping to meet constituent needs.

(b) (U) Coast Survey programs provide coastal navigation services and new electronic technologies to help mariners and pilots significantly reduce the risk of accidents and spills. In general, these representatives focus primarily on resolving charting and navigation questions, educating constituents on emerging charting technologies and their uses, and soliciting feedback on NOAA's navigation products and services from the commercial maritime industry.

(c) (U) Activities include:

- Meeting with local port authorities and harbormasters.
- Meeting with local marine pilots.
- Identifying locations requiring priority hydrographic surveys.
- Providing liaison on other issues such as predicted tides/currents.
- Addressing geographic information system needs.
- Providing outreach activities with the maritime community.
- Maintaining dialogue with oil companies, fishermen, commercial shippers and other commercial mariners.
- Improving and customizing nautical charts to satisfy specific regional needs.
- Providing expert advice to resolve local navigation safety issues that affect multiple agencies.
- Collaborating with local maritime professionals for updating the Coast Pilot.

- Working with regional constituents to define new navigation products such as the electronic nautical chart, raster nautical chart and "print on demand" charts.

(3) (U) For contact and other information about NOAA, visit:

- www.nauticalcharts.noaa.gov
- www.response.restoration.noaa.gov
- www.noaa.gov/wx.html

6. (U) Federal Emergency Management Agency (FEMA)

a. (U) ESF 3 (Public Works and Engineering), and ESF 10 (Oil and Hazardous Material Response) are categories under which debris-related activities are conducted during FEMA Mission Assignments. USACE is the lead agency for ESF 3. EPA is the lead agency for ESF 10.

b. (U) Technical Assistance Mission Assignments are available when the state, tribal, or local community lacks technical knowledge or expertise to accomplish an eligible task. Technical assistance may be authorized in anticipation of a declaration of a major disaster or emergency. Technical Assistance is usually fully funded by the federal government in accordance with provisions of the Stafford Act, which is subject to the procedures for determining eligibility administered by FEMA.

c. (U) Direct Federal Assistance Mission Assignments allow a federal agency to perform debris removal activities on behalf of the state or applicant. Direct Federal Assistance Mission Assignments apply only to Emergency Work (debris removal and emergency protective measures) and must meet the general FEMA eligibility criteria for Emergency Work. Federal agencies must comply with all applicable regulations, laws, policies, requirements, and procedures. For further guidance on FEMA debris removal policy, see the latest version of the Public Assistance Program and Policy Guide (PAPPG), which combines all Public Assistance (PA) policy into a single volume.

7. (U) National Transportation Safety Board (NTSB)

a. (U) A TSI may involve circumstances that would result in on-site safety investigation by the NTSB to identify causal factors and systemic safety issues. Salvage response may therefore need to be coordinated with NTSB investigations to ensure that evidence is preserved if possible, consistent with prevailing conditions, safety, and other pertinent factors.

8. (U) Interagency Agreements (IAA), Memorandum of Agreement (MOA)/Memorandum of Understanding (MOU)

   a. (U) Memorandum of Agreement between the Department of the Army and U.S. Coast Guard (October 1985). The MOA defines each agency's respective authorities for the marking and removal of sunken vessels and other obstructions to navigation. The MOA provides procedures to determine whether an obstruction is a hazard to navigation and procedures to determine the appropriate corrective actions to be taken by both parties.

   b. (U) Interagency Agreement (IAA) Between the United States Navy and the United States Coast Guard for Cooperation in Oil Spill Clean-Up Operations and Salvage Operations, 1980. The IAA established procedures for requesting and providing assistance between the two agencies and established reimbursement procedures and policies. SUPSALV is the Navy's designated point of contact for other agencies concerning salvage in U.S. waters (see paragraph 4 of this Tab).

   c. (U) Memorandum of Understanding between the American Salvage Association and U.S. Coast Guard Executing Marine Salvage and Firefighting Partnership, June, 2007. The purpose of the partnership is to strengthen the communication and working relationship between the Coast Guard and the marine and firefighting industry in part to enhance national maritime security preparedness and response and to promote timely, responsible and professional salvage response to marine casualties. The parties agreed to promote the partnership within their respective organizations and, as may seem best, involve their representatives at all levels in steps to be taken at the national, regional, or local levels. The parties agreed to interpret and implement the MOU in a manner that supplements (and not adversely affect) regulatory relationships.

   d. (U) *[ADD OTHER MOAS AND MOUS AS APPROPRIATE.]*

Tab C: Authorities

FEDERAL AUTHORITIES RELATED TO SALVAGE

1. (U) General. This Tab summarizes salvage-related authorities of some Federal organizations, but should not be considered a complete list. Authorities shown are subject to change and interpretation. Consultation through the pertinent ICS structures and participating agencies may be necessary to determine which authorities are applicable for the circumstances associated with the incident.

2. (U) U.S. Army Corps of Engineers (USACE).

   - USACE is authorized by Section 202 of Water Resources Development Act (WRDA) of 1976 (Public Law 94-587) to develop projects for the collection and removal of drift and debris from publicly maintained commercial boat harbors and from land and water areas immediately adjacent thereto.

   - The WRDA provides general authority for development of drift and debris removal projects. The Department of the Army does not currently support authorization of or budgeting for such projects.

   - Specific and limited local programs for continuing debris collection and disposal have been authorized by Congress for New York, Baltimore, and Norfolk Harbors; Potomac and Anacostia Rivers in the Washington, D.C. Metropolitan area; and San Francisco Harbor and Bay, California. These authorizations are on an individual basis, and the work is carried out as authorized at each locality as a separate, distinct project.

   - Sections 15, 19, and 20 of the River and Harbor Act of 1899 (as amended) authorize the USACE to remove sunken vessels or similar obstructions from navigable waterways. A navigable waterway is one that has been authorized by Congress and which the USACE operates and maintains for general (including commercial and recreational) navigation.

   - The Flood Control and Coastal Emergency Act (Public Law 84-99) authorizes USACE to provide assistance for debris removal from flood control works (structures designed and constructed to have appreciable and dependable effects in preventing damage by irregular and unusual rises in water level). Applicants for assistance must be an active participant in USACE's Rehabilitation and Inspection Program (RIP) prior to the flood event to be eligible for assistance.

   - USACE, under the National Response Framework, is designated the lead coordinator for ESF 3 (Public Works and Engineering). Under ESF 3, FEMA tasks the USACE to perform debris removal operations at the request of a state. This can include debris in the water outside the federally maintained channel if FEMA declares the situation eligible for assistance.

3. (U) U.S. Navy Director of Ocean Engineering and Supervisor of Salvage (SUPSALV).

- The Salvage Facilities Act (10 U.S.C. 7361 *et seq.*) gives the Navy broad discretion to provide necessary salvage support for both public and private vessels. This authorizes the provision of salvage facilities and services directly by Navy or via lease, sale or other contractual arrangement, which implies a standing role for SUPSALV as the "national salvage advisor."

- SUPSALV works on a reimbursable basis and is postured to accept all forms of government funding.

4. (U) Federal Emergency Management Agency (FEMA).

- FEMA is authorized in Sections 403, 407 and 502 of Reference (j) to provide assistance to eligible applicants to remove debris from public and private property or waters following a Presidential disaster declaration, when in the public interest.

- Removal must be necessary to eliminate immediate threats to lives, public health and safety; eliminate immediate threats of significant damage to improved public or private property or waters; or ensure the economic recovery of the affected community. The debris must be the direct result of the disaster and located in the disaster area, and the applicant must have the legal responsibility to remove the debris.

Tab D: Funding Considerations

FUNDING CONSIDERATIONS RELATED TO SALVAGE RESPONSE

1. (U) General. This Tab gives some funding considerations for salvage-related activities.

2. (U) U.S. Army Corps of Engineers (USACE).

   - Funding for operation and maintenance of these federally maintained navigable channels and waterways through USACE's Operations and Maintenance General Appropriation each year.

3. (U) Federal Emergency Management Agency (FEMA).

   - FEMA is authorized to; (1) reimburse applicants to remove eligible debris, or (2) through a Mission Assignment (MA) to another Federal agency (or upon request of the State) provide direct federal assistance or technical assistance when it has been demonstrated that state and local government lack the capability to perform or contract for the requested work.

   - Assistance provided by FEMA will be on a cost-share basis (at no less than 75% federal and 25% non-federal). In extreme circumstances, FEMA may provide up to 100% funding for a limited period of time.

4. (U) U.S. Coast Guard (USCG)

   a. (U) Funding is only available for a limited range of scenarios. Coast Guard units should ensure that the responsible party or vessel owner assumes responsibility for salvage costs when appropriate. Large commercial vessels and barges typically have Protection and Indemnity (P&I) Insurance to cover instances that result in salvage. This insurance provides coverage to ship owners and charterers against third-party liabilities encountered in their commercial operations. Death, injury or illness of passengers or crew, pollution, damage to cargo, and damage to docks and other installations are examples of incidents typically covered by P & I insurance. However, there are times when the CG must take responsibility to rectify a waterway. In such instances, possible sources of funding include:

      - The Oil Spill Liability Trust Fund (created by OPA 90) - for spills or threats of spills of oil or petroleum products.

      - Comprehensive Environmental Response, Compensation, and Liability Act (CERCLA) - for hazardous substance releases or threats of release.

      - Stafford Act - pursuant to a disaster declaration.

- Agency Funding in accordance with existing legislation.

b. (U) In some instances, there may not be authority or funding for the Coast Guard to take action. In those cases, COTPs should make every effort to engage either private organizations or agencies that do have the authority and capability to act.

Tab E: Salvage Assessments

GUIDANCE TO ASSESS SALVAGE RESPONSE NEEDS

1. (U) General. This Tab provides general guidance considerations for determining what is needed for response in a particular salvage situation. The authorities and responsibility for a given situation will be largely determined by answers to the following questions.

2. (U) Incident-Specific Planning. Incident-specific salvage response plans should, at a minimum, address the following issues/concerns:

   - What: Identify whether the object of the salvage is a vessel, debris, structure, or other. Identify the type of vessel/structure, whether there is dangerous cargo involved (e.g., CDCs, CBRNE, etc.), and the severity of the consequences of a discharge, explosion, etc.

   - Where: Identify the location, whether there is an impact on a federally maintained navigable channel, whether a hazard to navigation exists, whether the hazard causes a significant disruption to the MTS, and whether the salvage operation itself could cause a disruption of the MTS.

   - When: Several factors influence the timing and phasing of the salvage response, including whether a Stafford Act declaration is in effect for the incident (affects funding) and whether investigative bodies (e.g., NTSB, FBI/JTTF, state/ local agencies) require access to the scene (which would drive requirements for identifying, collecting, and preserving evidence, etc.).

   - How: The nature of the incident (e.g., structural collapse, explosion, collision/allision), possibilities of secondary hazards (e.g., explosions), weather, and other factors that may influence the timing and methods of response should be addressed in the plan.

   - Who: Identification of the Responsible Party of the vessel/cargo/structure that became a hazard and whether a salvor or other interested party is attempting to salvage the property. Identification of the Responsible Party is usually required, as part of the process of determining the responsibility for conducting/funding of salvage operations, and determining whether unknown hazards to salvage operations exist.

   - Why: An understanding of the reason(s) the event occurred (e.g., terrorist attack or other), which can influence the timing and methods of salvage response, highlight the risk to salvors/responders (e.g., whether other explosive devices or chemical could present a hazard to salvage personnel), the need to collaborate with other agencies and organizations in the response (e.g., to collect and preserve evidence), etc.

Tab F: Salvage Response Framework

SALVAGE RESPONSE FRAMEWORK

1. (U) General. This Tab provides a salvage response framework for determining and developing site-specific salvage plans. This Tab covers only some of the possible salvage-related scenarios, and does not create new requirements or Coast Guard policy with respect to salvage. Each situation is different, and may or may not fall within the scope of this Tab. Further, each salvage response is unique and requires flexibility and good communication between all participants to ensure success.

2. (U) Framework. The narrative immediately below explains the diagram depicting salvage planning and response decision-making on the following page.

   a. (U) Any salvage response will be characterized by the type of incident that requires it. The framework assumes that ICS will be implemented for incident management as indicated in the diagram, and that salvage response needed to ensure that waterways can support maritime commerce is a post-incident activity after initial responses to the incident (e.g., SAR) have been completed. Salvage response operations for planning purposes are considered an element of the short-term recovery phase (3-90 days post-incident).

   b. (U) The following progression provides an orderly approach to salvage planning:

      (1) (U) Step 1. Perform an assessment to determine what occurred and what is needed (if anything) in terms of a salvage response.

      (2) (U) Step 2. Primary responsibility for salvage response belongs to the Responsible Party (RP), and their insurance underwriters (if any). Determine if there is a RP or not, and whether or not the RP is capable of performing the necessary salvage response within an acceptable period, as determined by applicable rules and regulations. If so, then determine oversight responsibility within the IC/UC established in response to the incident, and coordinate oversight and support as may be appropriate, consistent with applicable jurisdiction and authority. If the RP is not capable of or willing to perform salvage as required, or there is no RP, then proceed to Step 3.

      (3) (U) Step 3. Determine the appropriate combination of authority and funding sources that are available to perform essential salvage response. Determine federal lead and supporting roles, the appropriate mix of roles and responsibilities when multiple authorities and funding streams are needed to conduct the salvage operation, and the necessary coordination/transition mechanisms to be used during the operation. Once authority and funding are identified, a salvage plan specific to the incident should be developed (see Tabs B through E). The incident-specific salvage plan should be prepared by technical specialists with the

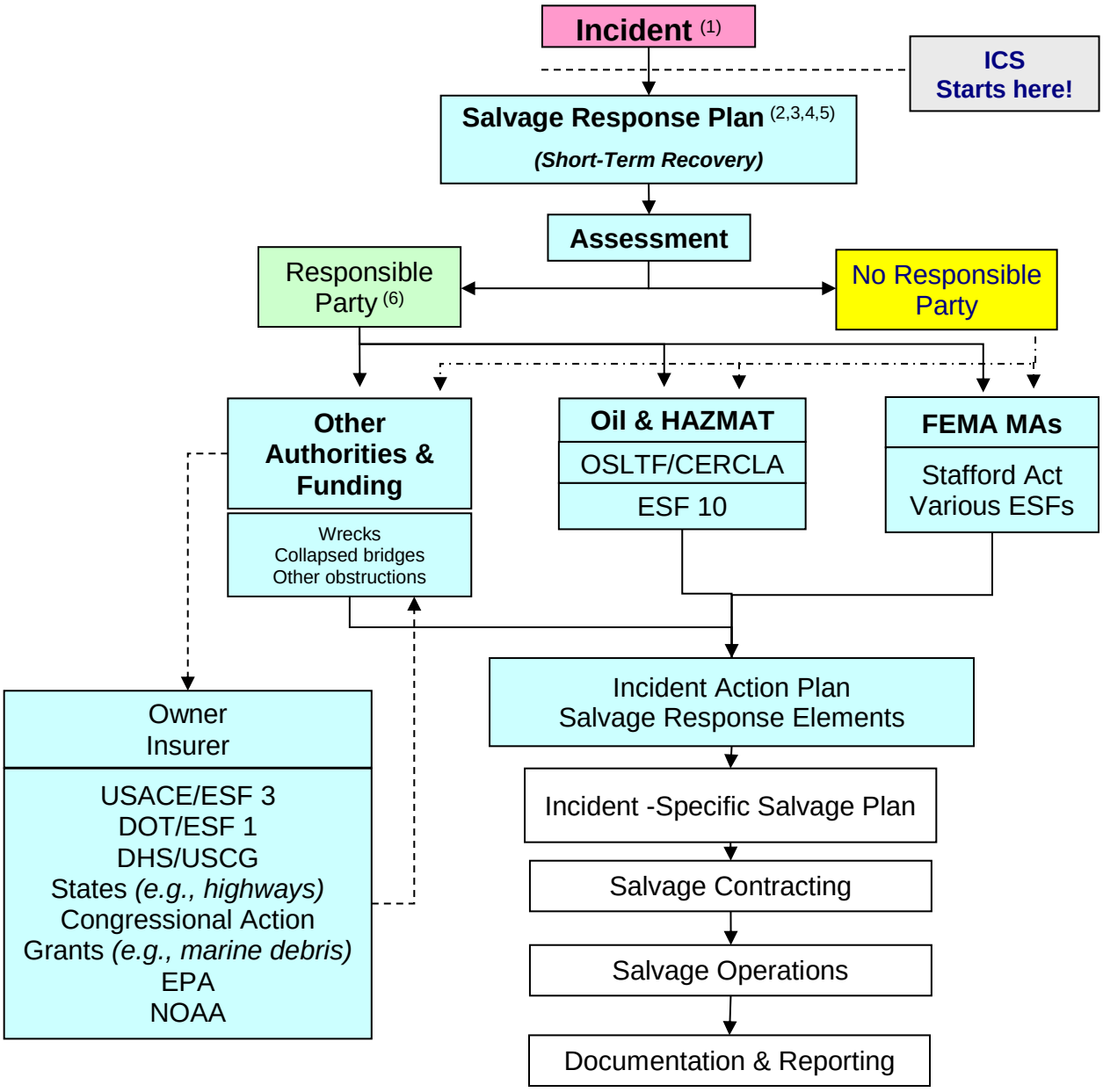
subject matter expertise necessary to conduct site-specific salvage assessments and to develop and implement procedures to resolve the obstruction(s) to navigation.

(4) (U) Step 4. Arrange for salvage support directly from government sources if appropriate (e.g., for salvage of assets owned by federal agencies), for contracting of commercial salvors, or if appropriate other marine service providers (e.g., for removal of marine debris other operations when marine salvage protocols are not applicable).

(5) (U) Step 5. The salvor will mobilize salvage response operations and conduct necessary salvage operations. The UC's technical specialists will provide oversight of RP salvage activity or manage salvage operations as appropriate to the situation.

(6) (U) Step 6. Plan and conduct documentation activities to provide a record of salvage response, and to track and monitor costs incurred by the federal government. Periodic reporting will be required to keep the UC posted on developments, and will follow the reporting schedule and protocols established for the incident.

SALVAGE RESPONSE FRAMEWORK



Notes:

1. Transportation Security Incident/other Transportation Disruption (e.g., manmade event, natural disaster).
2. Supporting plan to MTS Recovery during short-term recovery phase.
3. Relies on existing authorities & funding.
4. Applies to removal of obstructions to navigation from federally defined navigable waters…. "To ensure that the waterways are cleared and the flow of commerce through the United States ports is reestablished as efficiently and quickly as possible after a maritime transportation security incident .." per the SAFE Port Act.
5. Will be structured for all-hazard and all transportation disruption compatibility.
6. For the purpose of this notional diagram, Responsible Party includes the responsible party as defined by the Oil Pollution Act of 1990; the identified owner, operator, or lessee of a sunken or grounded vessel or wreck; and, the owner, operator or lessee of other obstructions in the waterway such as structures, train cars, and vehicles.

Tab G: Glossary of Acronyms

GLOSSARY OF ACRONYMS

1. (U) This Tab lists SRP-related acronyms.

AC	Area Committee
ACP	Area Contingency Plan
AMS	Area Maritime Security
AMSC	Area Maritime Security Committee
AMSP	Area Maritime Security Plan
AOI	Area of Interest
AOR	Area of Responsibility
AVP	Abandoned Vessel Program
CDC	Certain Dangerous Cargo
CBRNE	Chemical, Biological, Radiological, Nuclear, and Explosive
CERCLA	Comprehensive Environmental Response, Compensation, and Liability Act
C.F.R.	Code of Federal Regulations
CG	Coast Guard
CI/KR	Critical Infrastructure/Key Resource
COTP	Captain of the Port
DHS	Department of Homeland Security
DoD	Department of Defense
DOT	Department of Transportation
EEI	Essential Element of Information
ESF	Emergency Support Function
ESSM	Emergency Ship Salvage Material
FBI	Federal Bureau of Investigation
FEMA	Federal Emergency Management Agency
FMSC	Federal Maritime Security Coordinator
IAA	Interagency Agreement
IAP	Incident Action Plan
IC	Incident Command
ICP	Incident Command Post
ICS	Incident Command System
ILO	Infrastructure Liaison Officer
IMH	Incident Management Handbook
JFO	Joint Field Office
JTTF	Joint Terrorism Task Force
MA	Mission Assignment
MSC	Marine Safety Center

MTS	Marine Transportation System
MTSRU	MTS Recovery Unit
NASA	National Aeronautics and Space Administration
NAVAIR	Naval Air Systems Command
NAVSEA	Naval Sea Systems Command
NIMS	National Incident Management System
NOAA	National Oceanic and Atmospheric Administration
NRF	National Response Framework
NTSB	National Transportation Safety Board
NSFCC	National Strike Force Coordination Center
OPA 90	Oil Pollution Act of 1990
OSLTF	Oil Spill Liability Trust Fund
PEO	Program Executive Officer
POSSE	Program of Ship Salvage Engineering
PRC	Port Readiness Committee
RP	Responsible Party
SAFE Port Act	Security and Accountability for Every Port Act of 2006
SERT	USCG Marine Safety Center's Salvage Engineering Response Team
SME	Subject Matter Expert
SPAWAR	Space and Naval Warfare Command
SRP	Salvage Response Plan
SUPSALV	U.S. Navy Supervisor of Salvage and Diving
TSI	Transportation Security Incident
UC	Unified Command
U.S.	United States
USACE	United States Army Corps of Engineers
USCG	United States Coast Guard

Tab H: Local Marine Salvage Capabilities

LOCAL MARINE SALVAGE CAPABILITIES

[PREPARE AND INSERT A LIST OF LOCAL MARINE SALVAGE CAPABILITIES. ***THIS LIST IS A MANDATORY REQUIREMENT OF THE SAFE PORT ACT AND MUST BE INCLUDED.]***

ENCLOSURE (7) TO NVIC 09-02 CHANGE 5

GLOSSARY OF TERMS AND DEFINITIONS

Glossary of Terms and Definitions

AAR	After Action Report
ACP	Area Contingency Plan
AMS	Area Maritime Security
AMS Assessment	Area Maritime Security Assessment: An analysis that examines and evaluates the infrastructure and operations of a port taking into account possible threats, vulnerabilities, and existing protective measures, procedures, and operations.
AMSC	Area Maritime Security Committee
AMSP	Area Maritime Security Plan
AMSTEP	Area Maritime Security Training and Exercise Program
AOO	Area of Operations
AOR	Area of Responsibility
AWS	Alert Warning System
AWW	America's Waterway Watch
BOS	Breach of Security
CART	Common Assessment and Reporting Tool
C.F.R.	Code of Federal Regulations
CIKR	Critical Infrastructure Key Resources
CISA	Cybersecurity and Infrastructure Security Agency
COTP	Captain of the Port
CPPM	Contingency Planning and Preparedness Manual
CPT	Cyber Protection Team
CSO	Company Security Officer
CVI	Chemical Terrorism Vulnerability Information
DHS	Department of Homeland Security

DOD	Department of Defense
DOT	Department of Transportation
EEI	Essential Elements of Information: Quantitative and objective information that will be used to complete Status Report templates. These templates are designed to facilitate the collection and dissemination of consistent information regarding the status of the MTS following a significant disruption in Incident Areas and specified Non-Incident Areas.
EPA	Environmental Protection Agency
ESF	Emergency Support Function
FACA	Federal Advisory Committee Act
FEMA	Federal Emergency Management Agency
FMSC	Federal Maritime Security Coordinator
FOUO	For Official Use Only
FSA	Facility Security Assessment
FSO	Facility Security Officer
FSP	Facility Security Plan
GMDSS	Global Maritime Distress and Safety System
HSEEP	Homeland Security Exercise and Evaluation Program
IAA	Inter-Agency Agreement
IAP	Incident Action Plan
IC	Incident Command
ICC	Intelligence Coordination Center
IMH	Incident Management Handbook
Incident Area	A geographic area directly affected by an emergency situation requiring a response operation. The Incident Area may be a port, a waterway, or it may be an area proximate to a port where an incident will have, or is expected to have, a significant impact on the MTS.

IOC	Interagency Operations Center
ISPS	International Ship and Port Facility Security Code
IT	Information Technology
IUPA	Interagency Underwater Port Assessment
LES	Law Enforcement Sensitive
MARSEC	Maritime Security
MHS	Maritime Homeland Security
MCOP	Maritime Common Operating Picture
MOA	Memorandum of Agreement
MOU	Memorandum of Understanding
MSC	Marine Safety Center
MSM	Marine Safety Manual
MSRAM	Maritime Security Risk Analysis Model
MTEP	Multi-Year Training and Exercise Plan
MTS	Marine Transportation System
MTSA	Maritime Transportation Security Act
MTSRP	Marine Transportation System Recovery Plan
MTSRU	Marine Transportation System Recovery Unit: A unit of the Planning Section of the Incident Command System (ICS) established for every incident that significantly disrupts the MTS. This unit is primarily staffed by government personnel and is augmented by local marine industry expertise.
NCCIC	National Cybersecurity and Communications Integration Center
NIMS	National Incident Management System
NIPP	National Infrastructure Protection Plan
NOAA	National Oceanic and Atmospheric Administration

Non-Incident Area	Geographic areas outside of the Incident Area, including adjacent regions and/or the entire nation, where the MTS may be impacted by an incident, but may not require a response operation.
NPRN	National Port Readiness Network
NRC	National Response Center
NRF	National Response Framework
NSSE	National Special Security Event
NTAS	National Transportation Alert System
NTSB	National Transportation Safety Board
NVIC	Navigation and Vessel Inspection Circular
OPSEC	Operation Security
OT	Operational Technology
PAF	Public Access Facility
PCII	Protected Critical Infrastructure Information
PMP	Project Management Plan
PPD	Presidential Policy Directive
PRC	Port Readiness Committee
PRND	Preventative Radiological/Nuclear Detection
PSRA	Port Security Resiliency Assessment
PWCS	Ports, Waterways and Coastal Security
RBDM	Risk Based Decision Making
RCC	Regional Command Center
RAD/NUC	Radiation/Nuclear Detection
Recovery	Measures, operations and activities in incident areas that return the basic functionality of the MTS.

Response	Emergency measures, operations and activities in incident areas that address the immediate effects of an emergency situation. Among other things, response includes the early assessment of the impact of potential or actual transportation disruptions to the MTS caused by an emergency situation.
Restoration	The level or degree to which recovery efforts are capable of returning the MTS to pre-incident capacity. Measurement is based upon industry potential movement of cargoes.
Resumption of Commerce	Facilitating the movement of vessels, goods, commodities, and passengers following an incident that has significantly disrupted the MTS.
RIN	Risk Index Number
SAFE Port Act	Security and Accountability For Every Port Act (2006)
SBU	Sensitive but Unclassified
SERT	Salvage Engineering Response Team
Short Term Recovery	Measures, operations and activities in incident areas that return the basic functionality of the MTS. This process begins during Response and continues through the early stages of Resumption of commerce and trade.
SME	Subject Matter Expert
SOLAS	Safety of Life at Sea
SRP	Salvage Response Plan
SSA	Sector Specific Agency
SSAS	Ship Security Alert System
SSI	Sensitive Security Information
SUPSALV	U.S. Navy Supervisor of Salvage and Diving
Transportation Disruption	Any significant delay, interruption, or stoppage in the flow of trade caused by a natural disaster, heightened threat level, an act of terrorism, or any transportation security incident.
TSA	Transportation Security Administration
TSI	Transportation Security Incident

TSSP	Transportation Sector Specific Plan
TWIC	Transportation Worker Identification Credential
UC	Unified Command
USACE	U.S. Army Corps of Engineers
U.S.C.	United States Code
UTPP	Underwater Terrorism Preparedness Plan
VSO	Vessel Security Officer
VSP	Vessel Security Plan