NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 9-02, Change 1

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

Ref: (a) MSM Volume VII, Port Security, COMDTINST M16000.12 (series)
(b) Magnuson Act and Executive order 10173, as amended
(c) Ports And Waterways Safety Act (PWSA) of 1972
(d) Risk-Based Decision-Making, COMDTINST M16010.3 (series)
(e) COMDT COGARD Washington DC 172345 DEC 01
(f) PDD-63 Critical Infrastructure Protection
(g) HSPDD – 3 Homeland Security Advisory System
(i) Navigation and Vessel Inspection Circular No. 1-00, Guidance for the Establishment and Development of Harbor Safety Committees Under the Marine Transportation System (MTS) Initiative, COMDTPUB P16700.4
(j) Guidance for Coast Guard Coordination of MTS Improvement Efforts at the Regional and Local Level, COMDTINST M16010.9 (series)
(k) Interagency Commission on Crime and Security in U. S. Seaports, August 2000
(l) COMDT COGARD Washington DC R281216Z MAY 02/ALCOAST 258/02, G-CCS
(m) 49 CFR 1520 TSA Regulations: “Protection of Sensitive Security Information”
(n) CPPM, Volume III; Exercise Policy COMDTINST M3010.13 (series)
(o) Maritime Transportation Security Act, Public Law 107-295; 46 USCA §§ 70101 et. seq.

*NON-STANDARD DISTRIBUTION: Ba: Commandant (G-MP/G-MOC/M01/MSE/MW/OPD/OPL/OPF-3). Distributed by electronic means only.
1. **PURPOSE.** The purpose of this Circular is to 1) provide guidance to field commanders on the development of Area Maritime Security Committees and Area Maritime Security (AMS) Plans; 2) provide guidance on the responsibilities of the Captain of the Port (COTP) acting as the Federal Maritime Security Coordinator (FMSC); 3) provide a common template for the development of AMS Plans; and 4) address port security issues that are the shared responsibility of the port stakeholders and AMS Committees.

2. **ACTION.** Commanding Officers of Activities, Marine Safety Offices, and COTPs will give the guidance in this circular the widest dissemination to the maritime community and AMS Committee members. Formation of the AMS Committees and development of AMS Plans should follow the guidance provided in enclosures (1) through (3). This circular will be distributed by electronic means only. It is available on the World Wide Web at http://www.uscg.mil/hq/g-m/nvic/index.htm. Distribution by COTPs may be made by any practical method.

3. **DIRECTIVES AFFECTED.** NVIC 9-02 is revised to provide guidance on the Final Rules on Maritime Security, 33 CFR Subchapter H, and the Maritime Transportation Security Act (MTSA) of 2002. Enclosures (1) and (2) are replaced in their entirety. Enclosure (3), the Port Security Risk Assessment Tool, is unchanged and should continue to guide the FMSC in the development of AMS Assessments.

4. **BACKGROUND.**

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

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

   c. On November 25, 2002, the President signed into effect Public Law 107-295, the Maritime Transportation Security Act of 2002 (MTSA), that mandated the development of a new regulatory scheme for maritime security. The Coast Guard conducted extensive public outreach, including seven public meetings to request comment on the development of interim rules to implement the MTSA. More than
2,000 people representing a cross-section of the maritime community attended these meetings and provided extensive comments. The Coast Guard incorporated the public comment into the development of Six Temporary Interim Rules (TIR) that were published in the Federal Register on July 1, 2003. Following another public meeting and the receipt of 1,600 comments from the public, the TIRs were published as Final Rules on October 22, 2003.

5. DISCUSSION.

a. This revised circular provides guidance to FMSCs, on how to bring existing Port Security Committees (PSC) and Port Security Plans (PSP) into compliance with 33 CFR Subchapter H, pertaining to the establishment of AMS Committees and AMS Plans. For the purpose of this guidance, the term “area” is defined as a COTP zone. The term “FMSC” is used to designate the COTP when implementing the provisions of 33 CFR Subchapter H.

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

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

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

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

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

6. IMPLEMENTATION.

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

b. FMSC Responsibility

(1) FMSCs will use the enclosed guidelines to develop AMS Committees that conform to 33 CFR Subchapter H for Area Maritime Security and the MTSA. Confirmation that these committees have been chartered and established will be provided to Districts, Areas, and G-MP no later than January 31, 2004.

(2) Each FMSC will use the enclosed guidelines to develop an AMS Plan. These plans may include geographic sub-plans as annexes so long as the entire COTP zone is covered. Since the U.S. intends to rely on the approval of AMS Plans as the basis for its compliance with the Port Facility section of the ISPS Code, adherence to the AMS Plan submission schedule is essential in order to provide timely notification to IMO.

(3) AMS Plans will be submitted by the FMSC in an electronic format to their District Commander for review no later than April 1, 2004.

c. District Responsibility

(1) District Commanders will engage with MSO planners well before March 1, 2004, to ensure timelines are met. In doing so, they will provide any technical or drafting assistance needed at the field level.
(2) District Commanders will review all AMS Plans within their District based on the criteria found in enclosure (2), and forward the plans to their Area Commander no later than May 1, 2004.

d. Area Responsibility

(1) Area Commanders will review and approve all AMS Plans in accordance with the criteria found herein, and forward approved AMS Plans to G-MP no later than June 1, 2004.

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

DAVID S. BELZ
Assistant Commandant for Operations

Encl: (1) Guidance for Development and Management of AMS Committees
(2) Guidance for Development and Management of AMS Plans
(3) Port Level AMS Assessments (PSRAT)
NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 9-02, Change 1

Dec 15 2003

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

Ref: (a) MSM Volume VII, Port Security, COMDTINST M16000.12 (series)
(b) Magnuson Act and Executive order 10173, as amended
(c) Ports And Waterways Safety Act (PWSA) of 1972
(d) Risk-Based Decision-Making, COMDTINST M16010.3 (series)
(e) COMDT COGARD Washington DC 172345 DEC 01
(f) PDD-63 Critical Infrastructure Protection
(g) HSPDD – 3 Homeland Security Advisory System
(i) Navigation and Vessel Inspection Circular No. 1-00, Guidance for the Establishment and Development of Harbor Safety Committees Under the Marine Transportation System (MTS) Initiative, COMDTPUB P16700.4
(j) Guidance for Coast Guard Coordination of MTS Improvement Efforts at the Regional and Local Level, COMDTINST M16010.9 (series)
(k) Interagency Commission on Crime and Security in U. S. Seaports, August 2000
(l) COMDT COGARD Washington DC R281216Z MAY 02/ALCOAST 258/02, G-CCS
(m) 49 CFR 1520 TSA Regulations: “Protection of Sensitive Security Information”
(n) CPPM, Volume III; Exercise Policy COMDTINST M3010.13 (series)
(o) Maritime Transportation Security Act, Public Law 107-295; 46 USCA §§ 70101 et seq.

*NON-STANDARD DISTRIBUTION: Ba: Commandant (G-MP/G-MOC/MO-1/MSE/MW/OPD/OPL/OPF-3). Distributed by electronic means only.
1. **PURPOSE.** The purpose of this Circular is to 1) provide guidance to field commanders on the development of Area Maritime Security Committees and Area Maritime Security (AMS) Plans; 2) provide guidance on the responsibilities of the Captain of the Port (COTP) acting as the Federal Maritime Security Coordinator (FMSC); 3) provide a common template for the development of AMS Plans; and 4) address port security issues that are the shared responsibility of the port stakeholders and AMS Committees.

2. **ACTION.** Commanding Officers of Activities, Marine Safety Offices, and COTPs will give the guidance in this circular the widest dissemination to the maritime community and AMS Committee members. Formation of the AMS Committees and development of AMS Plans should follow the guidance provided in enclosures (1) through (3). This circular will be distributed by electronic means only. It is available on the World Wide Web at [http://www.uscg.mil/hq/g-m/nvic/index.htm](http://www.uscg.mil/hq/g-m/nvic/index.htm). Distribution by COTPs may be made by any practical method.

3. **DIRECTIVES AFFECTED.** NVIC 9-02 is revised to provide guidance on the Final Rules on Maritime Security, 33 CFR Subchapter H, and the Maritime Transportation Security Act (MTSA) of 2002. Enclosures (1) and (2) are replaced in their entirety. Enclosure (3), the Port Security Risk Assessment Tool, is unchanged and should continue to guide the FMSC in the development of AMS Assessments.

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

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

c. On November 25, 2002, the President signed into effect Public Law 107-295, the Maritime Transportation Security Act of 2002 (MTSA), that mandated the development of a new regulatory scheme for maritime security. The Coast Guard conducted extensive public outreach, including seven public meetings to request comment on the development of interim rules to implement the MTSA. More than
2,000 people representing a cross-section of the maritime community attended these meetings and provided extensive comments. The Coast Guard incorporated the public comment into the development of Six Temporary Interim Rules (TIR) that were published in the Federal Register on July 1, 2003. Following another public meeting and the receipt of 1,600 comments from the public, the TIRs were published as Final Rules on October 22, 2003.

5. DISCUSSION.

a. This revised circular provides guidance to FMSCs, on how to bring existing Port Security Committees (PSC) and Port Security Plans (PSP) into compliance with 33 CFR Subchapter H, pertaining to the establishment of AMS Committees and AMS Plans. For the purpose of this guidance, the term “area” is defined as a COTP zone. The term “FMSC” is used to designate the COTP when implementing the provisions of 33 CFR Subchapter H.

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

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

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

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

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

6. IMPLEMENTATION.

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

b. FMSC Responsibility

(1) FMSCs will use the enclosed guidelines to develop AMS Committees that conform to 33 CFR Subchapter H for Area Maritime Security and the MTSA. Confirmation that these committees have been chartered and established will be provided to Districts, Areas, and G-MP no later than January 31, 2004.

(2) Each FMSC will use the enclosed guidelines to develop an AMS Plan. These plans may include geographic sub-plans as annexes so long as the entire COTP zone is covered. Since the U.S. intends to rely on the approval of AMS Plans as the basis for its compliance with the Port Facility section of the ISPS Code, adherence to the AMS Plan submission schedule is essential in order to provide timely notification to IMO.

(3) AMS Plans will be submitted by the FMSC in an electronic format to their District Commander for review no later than April 1, 2004.

c. District Responsibility

(1) District Commanders will engage with MSO planners well before March 1, 2004, to ensure timelines are met. In doing so, they will provide any technical or drafting assistance needed at the field level.
(2) District Commanders will review all AMS Plans within their District based on the criteria found in enclosure (2), and forward the plans to their Area Commander no later than May 1, 2004.

d. Area Responsibility

(1) Area Commanders will review and approve all AMS Plans in accordance with the criteria found herein, and forward approved AMS Plans to G-MP no later than June 1, 2004.

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

DAVID S. BELZ  
Assistant Commandant for Operations

Enc
d:  (1) Guidance for Development and Management of AMS Committees  
(2) Guidance for Development and Management of AMS Plans  
(3) Port Level AMS Assessments (PSRAT)
ENCLOSURE (1) TO NVIC 9-02 CHANGE 1

GUIDANCE FOR DEVELOPMENT AND MANAGEMENT OF AREA MARITIME SECURITY (AMS) COMMITTEES
1. **PURPOSE.**

   a. The guidance provided in this enclosure is intended to assist the Federal Maritime Security Coordinators (FMSC) in establishing Area Maritime Security (AMS) Committees, and in transforming existing Port Security Committees (PSC) into AMS Committees by providing information and guidance on the purpose, structure, and conduct of AMS Committees.

2. **BACKGROUND.**

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

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

   c. Although the MTSA specifically waives the application of the Federal Advisory Committee Act (FACA), 5 U.S.C. App. Sec. 14, to the formation of AMS Committees, each AMS Committee is required to conform to certain provisions in the MTSA, and the procedures established in 33 CFR 103.300. In particular, 103.300 mandates a written charter for the formation of AMS Committees. Therefore, FMSCs who wish to transform existing PSCs into AMS Committees must ensure that they develop charters for those existing PSC that conform to 33 CFR 103.300.

3. **DISCUSSION.**

   a. **Establishment of AMS Committees**

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

      (2) Although the MTSA makes the establishment of AMS Committees optional, the Commandant has determined that AMS Committees are both necessary and desired as a means to develop meaningful security assessments and broad-based security plans that incorporate input from port stakeholders. Reflecting
the Commandant’s findings, and to facilitate the creation of AMS Committees, 33 CFR 103.300 provides that PSCs established prior to July 1, 2003, may be considered as AMS Committees if they conform to the procedures established by 33 CFR 103.300.

(3) Many ports have multiple PSCs, with some having as many as seven separate committees. Particularly in those COTP zones that encompass several existing geographically separate PSCs, or when one existing PSCs has a significantly large membership, FMSCs are encouraged to form executive steering committees to oversee existing PSCs. Those existing PSCs, in turn, may be viewed as subcommittees of the AMS Committee if the FMSC so chooses. This practice is intended to simplify membership requirements, as the more formal rules mandated by 33 CFR Part 103 would apply only to the executive steering committee. The use of, or option to use, executive steering committees will give the FMSC flexibility in issuing, or not issuing, designation letters to members of subcommittees. Additionally, members of subcommittees, unlike members of AMS Committees, may serve more than five-year terms. Some committees, such as the Harbor Safety Committees (HSC), already have subcommittees or ad hoc committees in place working on port security issues, and FMSCs may also choose to expand these HSCs to form AMS Committees so long as the Committees adhere to 33 CFR Part 103.

b. Purpose and responsibilities of the AMS Committees.

(1) The purpose of the AMS Committee is to assist and advise the FMSC in the development, review and update of an AMS Plan for its COTP zone. It is essential that the Committee, working with the FMSC, develop a plan that contemplates attacks upon its particular infrastructure that would most likely create a Transportation Security Incident (TSI) within its zone. In doing so, the AMS Committee should consider the MTS infrastructure defined in “An Assessment of the U. S. Marine Transportation System,” and in Presidential Decision Directive 63, “Critical Infrastructure Protection.”

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

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

c. Organization of AMS Committees.

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

(i) Federal Agencies:
- US Coast Guard (e.g., Groups, Air Stations, Small Boat Stations, VTS, MSSTs, Auxiliaries);
- Department of Defense (DOD);
- Nuclear Regulatory Commission (NRC);
- US Department of Agriculture (USDA);
- Environmental Protection Agency (EPA);
- Occupational Safety and Health Agency (OSHA);
- Federal Bureau of Investigation;
- Federal Emergency Management Agency (FEMA);
- Bureau of Customs and Border Protection (BCBP);
- Bureau of Immigration and Customs Enforcement (BICE);
- Transportation Security Administration (TSA);
- Army Corps of Engineers (ACOE);
- US Transportation Command (TRANSCOM);
- Military Sealift Command (MSC);
- Military Traffic Management Command (MTMC);
- Animal and Plant Health Inspection Service (APHIS);
- Maritime Administration (MARAD);
- Research and Special Programs Administration (RSPA);
- Federal Railway Administration (FRA);
- Federal Highway Administration (FHWA);
- Federal Transit Administration (FTA);
- Other government representatives, where appropriate.

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

(iii) Industry related agencies:
• Facility owners/operators;
• Terminal owners/operators;
• Trade organizations;
• Recreational boating organizations (Yacht Clubs, rowing clubs);
• Railroad companies;
• Trucking companies;
• Shipyards;
• Tow-boat operators;
• Marine exchanges;
• Industry organizations;
• Organized labor;
• Commercial fishing industry;
• Waterborne vendors & service providers (Harbor Tugs, Launch Services, Line Handlers, small ferry operators, water taxis);
• Other facilities within the port having waterside access, e.g., refineries, chemical plants, power plants.

(2) The MTSA, at 46 USCA 70112(3), requires that before appointing a member to a position on the AMS Committee, notice soliciting nominations for membership on that Committee shall be published in the Federal Register. Accordingly, Coast Guard Headquarters will publish notice each December. Interested parties will be directed to the nearest FMSC to apply. FMSCs shall ensure membership elections and appointments are timed in accordance with the Federal Register Notice each year. It is not expected that every AMS Committee will have a vacancy in every year. If, after the solicitation/application process is complete, a FMSC becomes aware of other individuals or sectors of the port industry that he/she believes should be part of the AMS Committee, it is up to the FMSC to solicit representation.
from those individuals or sectors. This may be done without any further requirement to publish a notice in the Federal Register. For example, it may be appropriate for the FMSC to solicit Federal Agency representatives outside the Federal Register process to ensure strong agency representation on the Committee. Also, for those members who may have already been designated in writing by the FMSC as members of AMS Committees, it is not necessary for these members to reapply for their positions.

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

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

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

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

(7) The FMSC shall designate a member of his/her staff as the Executive Secretary of the AMS Committee. The Executive Secretary shall be responsible for the administrative duties of the Committee, such as maintaining current designation letters, publishing meeting agendas, recording meeting minutes, and maintaining current editions of the AMS Plan, including digital versions. It is also the responsibility of the Executive Secretary to ensure that all committee records are properly maintained and designated as Sensitive Security Information (SSI) where appropriate.
(8) 46 USCA 70112(f) states that a member of a committee established under this section, when attending meetings of the committee or when otherwise engaged in the business of the committee (including AMS Committees and the National Maritime Security Advisory Committee) is entitled to receive compensation and travel or transportation expenses. The Department of Homeland Security has determined that persons serving on advisory committees within the Department shall not receive compensation. Historically, this is consistent with other Coast Guard Federal Advisory Committees; and as such, does not represent a change in policy. Accordingly, compensation for participation on AMS Committees shall be set at zero. For travel and transportation costs, the Coast Guard has determined that a rate of $1 will apply to members of AMS Committees, as the Committees will meet locally. FMSCs may include in the Committee charter a statement that members will forego transportation, travel and compensation costs associated with participation on the AMS Committee, and all members shall sign the charter to acknowledge the waiver of travel fees and compensation. If the FMSC determines that, due to unusual circumstances, it is necessary to pay travel for a designated AMS Committee member, the FMSC may authorize travel expenses from within current operating budgets.

(9) Until the AMS Plan is finalized, reviewed, and approved, it is expected that most AMS Committees will meet more frequently than required by the regulations. At a minimum, 33 CFR 103.300(4) requires that AMS Committees meet at least once in a calendar year, or when requested by a majority of the AMS Committee members. Meetings need not take place in person, and FMSCs may take advantage of telephone and video conferencing when in-person meetings are impractical.

d. Sensitive Security Information.

(1) Much of the work of the AMS Committee will involve handling Sensitive Security Information (SSI). The Coast Guard's procedures for handling SSI are published in COMDTINST 5510.5, Security Classification and Designation Policy for Port Security Assessments (PSA), Critical Infrastructure (CI) Listings, and Port Security Assessment Tools (PSRAT). Additionally, the Department of Homeland Security (DHS) is expected to release a rulemaking on SSI in the very near future. Policy guidance on designation and handling of SSI for the AMS Plan and AMS Committee is provided in enclosure (2). It was developed based on the rulemaking and COMDTINST 5510.5. The FMSC, in conjunction with the AMS Committee, is responsible for developing procedures to protect both SSI and classified information that is developed and used by the Committees.

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

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

(4) AMS Committee meeting minutes and records that are not designated as SSI may be made available to the public pursuant to the Freedom of Information Act. However, FMSCs shall ensure that all material designated as SSI, and all records of discussions of material designated as SSI, are protected from disclosure to the public. Enclosure (2) of this circular provides additional guidance on the handling of SSI materials.

(5) It is not anticipated that AMS Committees or Plans will discuss or contain information classified above the SSI designation. Classified materials incorporated into the AMS Plan should be prepared as separate documents, referenced in the unclassified plan, and handled and stored in accordance with proper security procedures. However, if the need arises to discuss information classified as Secret with members of the AMS Committee, the FMSC may request security clearances for those Committee members with whom the FMSC intends to share the information. By using the definition of employee under Executive Order 12968, the Coast Guard is permitted to sponsor and grant clearances for a select number of AMS Committee members. All requests of this nature should be forwarded to G-MPS and describe the number of clearances requested, and the specific reason why they are necessary.
Dear ____________:

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

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

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

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

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

Sincerely,

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

Enclosure: Acceptance of Appointment Letter

Copy: ____________ Committee
Commander, ____ Coast Guard District (m)
Acceptance of Appointment
to the
____________________ Committee

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

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

This __ day of ________________, 20__.

[Appointee’s Name]
Letter of Appointment to the ______ AMS Committee

Dear _________________

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

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

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

Sincerely,

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

Enclosure: Committee Charter

Copy: ______________ Committee Chair
       Commander, ______ Coast Guard District (m)
ENCLOSURE (2) TO NVIC 9-02 CHANGE 1

GUIDANCE FOR DEVELOPMENT OF AREA MARITIME SECURITY PLANS
1. **PURPOSE.**

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

2. **BACKGROUND.**

a. The first step in developing an AMS Plan was the completion by the FMSCs of the AMS Assessment using the Port Security Risk Assessment Tool (PSRA T), which was designed to internally assess vulnerabilities based on national security priorities. In creating its AMS Plan, each AMS Committee should review and comment upon the PSRA T, and any other relevant assessments that may have been done. Building upon those nationally focused assessments, the AMS Committee’s assessment for its particular COTP zone should maintain a local emphasis and focus on priorities set by the community. Each FMSC should consider the PSRA T results when developing strategies for deploying resources within his or her zone. Future security assessments will allow for adjustments to the AMS Plan based on changing security needs and threats.

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

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

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

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

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

3. DISCUSSION

a. The AMS Plan developed by the FMSC and the AMS Committee must address the entire COTP zone, but the FMSC has discretion on how to present the geographic area covered within the Plan. This flexibility is necessary since it may be that different geographic areas within the COTP zone have significantly disparate security
concerns and protection strategies. In those cases, the FMSC may elect to complete the template provided in enclosure (2) for each geographic region within the zone. If the COTP chooses to compile multiple plans, the standard template and numbering system will still apply, and multiple geographic plans will be brought under the cover of a single AMS Plan. Conversely, some FMSCs may determine that certain areas within his or her COTP zone have such similar security concerns and protection strategies, e.g., Western Rivers, that he or she elects to combine different areas under one regional AMS plan.

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

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

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

e. The AMS Plan is primarily considered an awareness, preparedness, and prevention plan. While it does contain some response planning elements, it is not considered a response plan. Where overlaps occur with other existing crisis management plans, linkages and references should be made in the AMS Plan.

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

g. As the lead Federal Agency for maritime homeland security, the Coast Guard is responsible to accomplish the effective management and dissemination of critical security data. Accordingly, all efforts to compile security plan data in an electronic format should be made.
h. The areas of the AMS Plan that are deemed most critical are:

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

i. Best (Recommended) Practices:

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

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

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

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

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

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

(6) **Imagery:** If imagery is used in the AMS Plan, it is best to use ortho-rectified (direct overhead) photos. This will permit the introduction of Geographic Information System (GIS) data as overlays in the future.
4340 Operational Security (OPSEC) Measures ................................................................. 27
4400 MARSEC Level 2 ..................................................................................................... 28
4410 Standard Security Procedures for MARSEC Level 2 ............................................ 28
4420 Roles, Resources, Authorities, and Responsibilities ........................................... 28
4430 Physical Security Measures .................................................................................... 28
4440 Operational Security Measures ............................................................................ 29
4500 MARSEC Level 3 ..................................................................................................... 29
4510 Standard Security Procedures for MARSEC Level 3 ............................................ 29
4520 Roles, Resources, Authorities, and Responsibilities ........................................... 29
4530 Physical Security Measures .................................................................................... 29
4540 Operational Security Measures ............................................................................ 30
4600 Public Access Facility .......................................................................................... 30
4610 Designation of Public Access Facilities (PAF) ....................................................... 30
4620 Withdrawal of Designation .................................................................................... 31
4700 Maritime Worker Credentials (reserved) .............................................................. 31
5000 PREPAREDNESS FOR RESPONSE .................................................................... 31
5100 Introduction ............................................................................................................. 31
5110 Procedures for responding to suspicious activity .................................................. 32
5120 Procedures for responding to breaches of security .............................................. 32
5200 Transportation Security Incident (TSI) ................................................................. 32
5210 Procedures for Notification ................................................................................... 32
5220 Incident Command Activation ............................................................................. 32
5230 Threats That Do Not Rise to the Level of a TSI .................................................... 32
5300 Most Probable Transportation Security Incident ................................................... 33
5310 Identify Command Structure With Assigned Roles (ICS Flowchart) ...................... 33
5320 Procedure For Responding To TSI ...................................................................... 33
5330 Linkage With Applicable Federal, State, Port, & Local Plans ............................... 33
5400 Maritime Security Exercise Requirements ........................................................... 34
5410 Purpose of Exercise Program .............................................................................. 34
5420 Goals of the AMS Plan Exercise Program ......................................................... 35
5430 Exercise Cycle ....................................................................................................... 35
5440 Scheduling And Design ...................................................................................... 35
5450 Consideration Of Equivalent Response ............................................................. 36
5460 Recordkeeping ..................................................................................................... 36
5470 Linkages Between Family Of Plans Within The Area ......................................... 36
6000 CRISIS MANAGEMENT AND RECOVERY ......................................................... 36
6100 Introduction ............................................................................................................. 36
6200 Procedures to Maintain Infrastructure ................................................................... 37
6300 Procedures for Recovery of MTS ......................................................................... 37
7000 COMPLIANCE MEASURES .................................................................................. 37
8000 PLAN DOCUMENTATION AND MAINTENANCE ............................................... 37
8100 Initial Plan Review and Comment ......................................................................... 37
8110 Procedures For Continuous Review And Update Of AMS Plans ....................... 37
8120 Procedures for Continuous Review and Update of the AMS Assessment ............. 38
9000 APPENDICES (OPTIONAL) ...................................................................................... 38
9100 Area Maritime Security (AMS) Committee Members .......................................... 39
9200 Charts and Maps of Port Areas ............................................................................. 39
9300 Port Operations and Infrastructure ...................................................................... 39
9400 Risk-Based Scenarios ............................................................................................ 39
9500 Dangerous Cargos for Security Planning ............................................................ 39
9600 Glossary of Terms ................................................................................................ 39
1000 AREA MARITIME SECURITY

1100 Purpose

[No additional comments required.]

(a) The Area Maritime Security (AMS) Committee for [Blank] has created this AMS Plan. It is designed to deter, to the maximum extent possible, a transportation security incident (TSI). This Plan will define Federal State and local governments’ obligations, and the contributions and responsibilities of other port stakeholders, to the Maritime Homeland Security (MHS) mission.

(b) A primary purpose of the AMS Plan is to provide a framework for communication and coordination amongst port stakeholders and law enforcement officials, and to identify and reduce vulnerabilities to security threats in and near the Maritime Transportation System (MTS). It is designed to capture the information necessary to coordinate and communicate security procedures at each MARSEC Level, complement and encompass facility and vessel security plans within its particular COTP zone, and ultimately be integrated into the National Maritime Security Plan. Pursuant to the AMS Plan, MTS stakeholders will take certain actions contingent upon changes in MARSEC Levels and develop unified preparedness strategies to deter and respond to security incidents.

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

   (1) An incident affecting a particular mode of transportation or inter-modal structure that significantly disrupts normal operations or may result in closure for a significant time period of a key terminal, waterway, or part of the MTS;

   (2) An actual incident, such as an explosion, MTS blockage, release of a Weapon of Mass Destruction (WMD), hijacking, etc.

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

1200 Captain of the Port (COTP) Letter of Promulgation

1210 Record of Changes

1300 Authority

[No additional comments required.]

(a) Section 102 of the Maritime Transportation Security Act of 2002 (MTSA), P.L. 107-295, codified at 46 USC §§ 70101 –70117, mandates the development
of a National Maritime Transportation Security Plan, Area Maritime Security Plans, and Facility and Vessel Security Plans. The Coast Guard is designated as the Lead Federal Agency (LFA) responsible for implementation of the MTSA. The COTPs, acting as Federal Maritime Security Coordinators (FMSC), are responsible for developing AMS Plans with advice from AMS Committees.

1310 Federal Maritime Security Coordinator (FMSC)

[No additional comments required.]

(a) The COTP (List USCG unit and area/zone for this Plan) is designated as the FMSC, charged with the responsibility of establishing an AMS Committee and developing an AMS Plan. These security responsibilities are in addition to key responsibilities for traditional Coast Guard missions and are fundamental to the success of the maritime homeland security program. To accomplish the goals outlined in the Coast Guard’s Maritime Strategy for Homeland Security, the FMSC must rely on fellow Federal, State and local representatives, and other maritime area partners to assist whenever possible.

1400 Scope

[No additional comments required.]

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

(b) The plans required by 33 CFR Parts 104, 105, and 106 will provide the foundation of the overarching AMS Plan. However, the AMS Plan must extend beyond the required facility and vessel security plans, and develop strategies to reduce the vulnerabilities of the weakest elements of the port, including those vessels, facilities and infrastructure that are not regulated under 33 CFR Parts 104, 105 and 106.

1500 Suppositions

[No additional comments required.]

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

(1) Ports are very open and may be susceptible to a TSI, which may occur at any time with little or no warning.

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

(3) Maintaining continuity of operations and facilitating commerce in the port area is a critical consideration.
(4) Security must be maintained during response and crisis management incidents.

(5) It is in the best interest of the United States to increase port security by establishing and improving communications among law enforcement officials responsible for port security.

(6) Each entity directly or indirectly involved with the MTS will participate with the AMS Committee to increase awareness and enhance prevention of illegal acts.

(7) The National Oil and Hazardous Material Contingency Plan, National Response Plan, and other response plans will be activated for the purpose of response and crisis management due to a TSI.

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

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

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

### 1600 Situation

*No additional comments required.*

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

### 1610 Physical Characteristics

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

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

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

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

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

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

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

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

1620 Economic Characteristics

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

(1) Types of industry:
(2) Major inter-modal connectors:
(3) Major cargos:
(4) Recent economic data:

1630 Ports, Charts and Maps

[Port charts and maps will be included in the appendices.]
must detail the threats, vulnerabilities, and consequences associated with each port area within a COTP zone. This requirement may be met using the Risk-Based Decision-Making methodologies developed by the Coast Guard or other appropriate Risk Based Decision Making Tools.

(3) Integrating and/or amending existing security assessments of maritime facilities using agreed upon criteria.

(4) Developing information sharing procedures for threat warnings, response, intelligence gathering, and threat assessment among public and private entities.

(5) Soliciting stakeholder recommendations for continuing improvements of AMS measures.

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

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

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

2300 Charter

[Insert copy of AMS Committee Official Charter here]

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

2310 Committee Structure and Procedural Rules

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

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

(b) The FMSC will designate a member of his/her staff as the Executive Secretary of the AMS Committee. The Executive Secretary will be responsible for the administrative duties of the Committee, such as the designation of members, publishing meeting agendas, taking of meeting minutes, and maintaining current editions of the AMS Plan, including digital versions. The Executive Secretary is also responsible for ensuring that all committee records are properly maintained and designated as SSI as appropriate.

(c) Standing Committees will be designated in the charter and ad hoc committees may be developed on an as-needed basis.
(d) The AMS Committee will meet at least once in a calendar year or when requested by the FMSC or a majority of AMS Committee members. Records of these meetings may be made available to the public upon request. However, FMSCs will ensure that all material designated as SSI will be protected from disclosure to the public.

(e) Only those members who have been determined by the FMSC to be “Covered Persons” with a “need to know” will be given AMS Committee records that contain SSI material. Section 3500 of this Plan provides additional guidance on the handling of SSI materials.

2320 Relationship to Other Committees

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

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

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

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

(4) Other committees as appropriate.

3000 AWARENESS

3100 Introduction

[Include an explanation of “maritime situational awareness.”]

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

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

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

(a) When depicting Federal, State and local security and law enforcement jurisdictional boundaries and areas of responsibility, first, second and third tier response agencies will be addressed separately in the AMS Plan. A description of each agency’s individual location and capability will greatly enhance the Committee’s ability to determine which resources with what capacities, and how many of each, may respond to a TSI.
(b) Agencies are tiered as follows:

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

(2) Second level agencies are those with special recovery and containment capabilities for dealing with hazardous materials, rough terrain or underwater search and recovery, and other agencies having excavation or heavy equipment capabilities.

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

(c) Where a geographic information system (GIS) already exists, it is recommended that separate agency jurisdictional boundaries be portrayed on maps or charts in an overlay fashion. If possible, the portrayal will extend outside the AMS Committee's COTP zone to reveal other neighboring agencies or elements that may be involved both routine and crisis situations.

3300 Area Maritime Security (AMS) Assessment

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

(a) This AMS Plan is prepared based on an AMS Assessment, which is a risk-based analysis of the port or ports. The Coast Guard has developed a process that consists of five steps more fully outlined in enclosure (3).

(b) The steps are:

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

3310 Maritime Security Assessment Report

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

3400 Communications

[No additional comments required]

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

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

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

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

3410 Communication of Security Information

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

3410.1 Communication With the Public

[The Plan will document what means of communications will be used in emergency and non-emergency situations to communicate security information related to the maritime environment with the general public.]

(a) The public as a whole must be notified of possible actions or operations that might affect it. There are a variety of systems that may be used to communicate information on restrictions, closures, and activities that are exclusionary or restrictive in nature, including the Emergency Broadcast System, Community Awareness and Emergency Response (CAER) network, and State and local emergency management offices. The AMS Committee will designate a sub-committee or working group to develop this communication process and facilitate the exchange of security information.

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

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

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

3410.2 Communications With Waterway Users

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

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

3410.3 Communications With Commercial Vessels

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

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

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

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

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

(4) **Ship Security Alert System.** SOLAS Regulation XI-2/6 requires certain vessels to be outfitted with a ship security alert system (SSAS), which allows the vessel to covertly signal a competent authority that the security of the ship is under threat or has been compromised. Contracting Governments of foreign flagged vessels are required to immediately forward all SSAS transmissions from vessels within, or bound for, U.S. waters to the U.S. Coast Guard. Notification and response procedures to a SSAS alert shall be included within AMS plans. Notifications to Federal, State and local law enforcement agencies may be the primary response to a ship security alert. Field guidance on SSAS applicability, and technical guidance on the implementation of SOLAS Regulation XI-2/6, is under development.

### 3410.4 Communications With Facilities

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

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

3410.5 Communicating with Companies

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

3420 Security Reporting

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

(a) The National Response Center (NRC) will act as the fusion center for all security information required by 33 CFR 101.305, and serve as a conduit of information to and from consequence mitigation and law enforcement organizations. This includes reports of suspicious activity and actual security breaches that do not result in a TSI, which normally will require simultaneous notification to local law enforcement authorities. In addition, facilities or individuals may contact the FMSC directly with such information. The reports and information garnered as a result of follow-on investigations will formulate intelligence and threat information that can be used to adjust security conditions throughout the country. TAB C identifies methods that can be used for security reports of suspicious behavior and breaches of security.

3420.1 Procedures for reporting suspicious activity

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

(a) Quick Response Cards (QRC) may be used as an effective and efficient tool to collect important information, including reports of suspicious activities, during periods of heightened awareness, security breaches, and potential or actual TSIs. When used properly, the QRC eliminates confusion and ensures all necessary information is captured. The subject matter covered, or title, may be kept general, but specificity should be included in the body of the document. The QRC should be tailored to fit the needs of the user, but at a minimum, must include a brief introduction or instructions, ample space to collect all appropriate information, and important points of contact, incident follow up procedures, and applicable references. Several examples are provided in TAB C.
3420.2 Procedure for reporting breaches in security

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

3430 MARSEC Directives

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

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

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

3430.1 Procedures for communicating MARSEC Directives

[The AMS Plan will include detailed procedures on the dissemination of MARSEC Directives, including who will grant access to MARSEC Directives, to whom MARSEC Directives will be issued, and a means for tracking which persons have been given access to what MARSEC Directives.]

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

(b) The MARSEC Directives will be individually numbered, and will be assigned to a series that corresponds with the Part of 33 CFR subchapter H to which the MARSEC Directive refers. For example, the first MARSEC Directive addressing a new requirement for vessels regulated under Part 104 of 33 CFR subchapter H would be identified as “MARSEC Directive 104-01.”
Upon receiving notice that a new MARSEC Directive has been issued, affected entities must contact or be contacted by their local FMSC (or, if appropriate, their District Commander) to receive a copy of the MARSEC Directive. The FMSC or District Commander will confirm, prior to distributing the MARSEC Directive, that the requesting entity is a "Covered Person" with a "need to know." The requesting entity must confirm to the FMSC through the use of a standard non-disclosure form that it will safeguard the MARSEC Directive as SSI. A standard non-disclosure form is provided in TAB D.

3430.2 Procedures for responding to MARSEC Directives
[The AMS Plan will identify procedures for receiving notice of compliance with MARSEC Directives, and for verifying that all entities affected by the MARSEC Directives are in compliance. Additionally, the Plan will include general procedures for dealing with entities that request equivalent security measures or waivers.]

(a) Once a MARSEC Directive has been issued, it is the responsibility of the affected entities to confirm compliance with the Directive to the local FMSC or District Commander, as appropriate, and specify the methods by which the mandatory measures in the directive have been, or will be, met. In some cases, recipients may elect to submit proposed equivalent security measures to the local FMSC or District Commander, as appropriate.

3430.3 Role of the Area Maritime Security (AMS) Committee
[The Plan will identify the role of the AMS Committee in communicating MARSEC Directives.]

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

(b) In anticipation of providing assistance in the distribution of MARSEC Directives, the AMS Committee should develop protocols and procedures addressing how it will ensure that Directives are received in a timely manner, and the means by which it will document compliance with all MARSEC Directives.

3440 MARSEC Levels
[AMS Plans must make clear the link between the MARSEC Levels and the HSAS Threat Conditions, and who sets MARSEC Level.]
(a) The Coast Guard has developed a three tiered system of MARSEC Levels consistent with the Department of Homeland Security’s HSAS. The international community is also using a three-tiered alert system that is consistent with the MARSEC levels used by the Coast Guard.

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

1. MARSEC Level 1 applies when HSAS Threat Conditions Green, Blue, and Yellow are set.
2. MARSEC Level 2 corresponds to HSAS Threat Condition Orange.
3. MARSEC Level 3 corresponds to HSAS Threat Condition Red.

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

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

(e) MARSEC changes will be triggered under limited circumstances and usually in conjunction with elevation of HSAS levels, such as when the threat that prompted a change in the HSAS Threat Condition also imperils a component of the MTS. However, there will also be instances where the HSAS Threat Condition is elevated for threats unrelated to the MTS, or where, after the HSAS Threat Condition is elevated, it becomes clear that the MTS is not a target. In these instances, the Commandant may set MARSEC Levels below the equivalent HSAS Threat Condition. Furthermore, the Commandant may choose to raise the MARSEC Level at only specific ports in response to the elevated HSAS Threat Condition instead of requiring all ports nationwide or on a particular coast to elevate their protective measures. An example of where this might occur includes ports where military load-outs occur or at ports that are considered strategically important.
3440.1 Procedures to Communicate Changes in MARSEC Levels

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

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

(b) Changes in MARSEC Levels will be announced and obtained in the most expeditious means possible, preferably through a Broadcast Notice to Mariners or other existing mechanisms of communications (e.g., maritime exchanges, VTS, VTIS programs). Whatever means used, it will be sufficient to provide timely and adequate notice to vessels and facilities regulated under 33 CFR Part 104, 105, and 106.

3440.2 Notification of MARSEC Level Attainment

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

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

3440.3 Role of Area Maritime Security (AMS) Committee

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

3500 Sensitive Security Information

[This section governs the maintenance, safeguarding, and disclosure of AMS Plan information, and other records and information, that have been designated as Sensitive Security Information (SSI), as defined in paragraph 3510 of this template. This section does not apply to the maintenance, safeguarding, or disclosure of classified national security information, as defined by Executive Order 12968, or to other sensitive unclassified information that is exempt from]
3510 Information Designated as Sensitive Security Information

[No additional comments required.]

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

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

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

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

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

(1) Security programs and contingency plans. Any security program or security contingency plan issued, established, required, received, or approved by DHS, including:

   (i) Any vessel, maritime facility, or port area security plan required or directed under Federal law;

   (ii) Any national or area security plan prepared under 46 U.S.C. 70103; or


(2) Security Directives. Any Security Directive or order:

   (i) Issued by TSA under 49 CFR §§ 1542.303 or 1544.305, or other authority;

   (ii) Issued by the Coast Guard under the Maritime Transportation Security Act, 33 CFR Part 6, or 33 U.S.C. 1221 et seq. related to maritime security; or

   (iii) Any comments, instructions, and implementing guidance pertaining thereto.

(3) Information Circulars. Any notice issued by DHS regarding a threat to maritime transportation, including:

   (i) Any Information Circular issued by TSA under 49 CFR §§ 1542.303, § 1544.305, or other authority; or
(ii) Any Navigation or Vessel Inspection Circular issued by the Coast Guard related to maritime security.

(4) **Performance specifications.** Any performance specification and any description of a test object or test procedure, for:

(i) Any device used by the Federal Government or any other person pursuant to any MTS requirements of Federal law for the detection of any weapon, explosive, incendiary, or destructive device or substance; or

(ii) Any communications equipment used by the Federal Government or any other person in carrying out or complying with any MTS requirements of Federal law.

(5) **Vulnerability assessments.** Any vulnerability assessment directed, created, held, funded, or approved by the DHS, or that will be provided to DHS in support of a Federal security program.

(6) **Security inspection or investigative information.** Details of any security inspection, or investigation of an alleged violation of MTS requirements of Federal law that could reveal a security vulnerability, including the identity of the Federal special agent or other Federal employee who conducted the inspection or audit.

(7) **Threat information.** Any information held by the Federal Government concerning threats against transportation or transportation systems, and any sources or methods used to gather or develop threat information, including threats against cyber infrastructure.

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

(i) Security measures or protocols recommended by the Federal Government;

(ii) Information concerning the deployments, numbers, and operations of Coast Guard personnel engaged in maritime security activities, to the extent it is not classified national security information.

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

(i) Any procedures, including selection criteria, and any comments, instructions, and implementing guidance pertaining thereto, for screening of persons, accessible property, checked baggage, U.S. mail, stores, and cargo conducted by the Federal Government or any other authorized personnel;

(ii) Any information or sources of information used by a passenger or property screening program or system, including an automated screening system;
(iii) Detailed information about locations at which particular screening methods or equipment are used;

(iv) All security screener tests and scores of such tests;

(v) Performance or testing data from security equipment or screening systems;

(vi) Any electronic image shown on any screening equipment monitor, including threat images and descriptions of threat images for threat image projection systems.

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

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

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

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

- (i) Prepared by DHS; or
- (ii) Prepared by a State or local government agency and submitted by the agency to DHS.

(13) **Systems security information.** Any information involving the security of operational or administrative data systems operated by the Federal Government that have been identified by the DHS as critical to maritime transportation safety or security, including automated information security procedures and systems, security inspections, and vulnerability information concerning those systems.

(14) **Confidential business information.**
(i) Solicited or unsolicited proposals received by DHS, and negotiations arising from the same, to perform work pursuant to a grant, contract, cooperative agreement, or other transaction, but only to the extent that the subject matter of the proposal relates to MTS measures;

(ii) Trade secret information, including information required or requested by regulation or Security Directive, obtained by DHS in carrying out MTS responsibilities; and

(iii) Commercial or financial information, including information required or requested by regulation or Security Directive, obtained by DHS in carrying out MTS responsibilities, but only if the source of the information does not customarily disclose it to the public.

(15) Research and development. Information obtained or developed in the course of research related to MTS activities, where such research is approved, accepted, funded, recommended, or directed by the DHS, including research results.

(16) Other information. Any information not otherwise described in this section that the DHS determines is SSI under 49 U.S.C. 114(s). Upon the request of another Federal agency, the DHS may designate information as SSI not otherwise described in this section.

3520 Covered Persons

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

3520.1 Designation as a Covered Person.

(a) The following may be designated as a Covered Person:

1. Every owner, charterer, or operator of a vessel, including foreign vessel owners, charterers, and operators required to have a security plan under Federal or international law;

2. Every owner or operator of a maritime facility required to have a security plan under the Maritime Transportation Security Act, (Pub.L. 107-295), 46 U.S.C. 70101 et seq., 33 CFR Part 6, or 33 U.S.C. 1221 et seq.;
3. Any person performing the function of a computer reservation system or global distribution system for cruise line passenger information;

4. Any person participating in the National or an area security committee established under 46 U.S.C. 70112, or a Port Security Committee;

5. Any industry trade association that represents Covered Persons and has entered into a non-disclosure agreement (TAB D) with the DHS;

6. DHS;

7. Any person conducting research and development activities that relate to MTS and are approved, accepted, funded, recommended, or directed by DHS;

8. Any person who has access to SSI, as specified in paragraph 3540;

9. Each person employed by, contracting with, or acting for a Covered Person, including a grantee of DHS, and including a person formerly in such position;

10. Each person for which a vulnerability assessment has been directed, created, held, funded, or approved by the DHS, or that has prepared a vulnerability assessment that will be provided to DHS in support of a Federal security program;

11. Each person receiving SSI under paragraph 3540.

3530 Restrictions on the Disclosure of SSI.

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

(1) Take reasonable steps to safeguard SSI in that person’s possession or control from unauthorized disclosure. When a person is not in physical possession of SSI, the person must store it in a secure container, such as a locked desk or file cabinet or in a locked room;

(2) Disclose or otherwise provide access to SSI only to Covered Persons who have a “need to know”, unless otherwise authorized in writing by the Commandant of the Coast Guard, or the Secretary of DHS;

(3) Refer requests by other persons for SSI to TSA or the applicable component or agency within DHS;

(4) Mark SSI as specified in paragraph 3550; and

(5) Dispose of SSI as specified in paragraph 3580.

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

(2) Inform the sender of the record that the record must be marked as specified in paragraph 3550.

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

3540 Persons with a "Need to Know".

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

(1) When the person requires access to specific SSI to carry out MTS activities approved, accepted, funded, recommended, or directed by DHS;

(2) When the person is in training to carry out MTS activities approved, accepted, funded, recommended, or directed by DHS;

(3) When the information is necessary for a person to supervise or otherwise manage individuals carrying out MTS activities approved, accepted, funded, recommended, or directed by the DHS;

(4) When the person needs the information to provide technical or legal advice to a Covered Person regarding MTS requirements of Federal law;

(5) When the person needs the information to represent a Covered Person in connection with any judicial or administrative proceeding, except in the case of an individual serving as litigation counsel who is not a direct employee of the Covered Person, the person has a "need to know" only if:

(i) In the judgment and sole discretion of the DHS, access to the SSI is necessary for adequate representation of the Covered Person in the proceeding. The DHS may make the individual’s access to the SSI contingent upon satisfactory completion of a security background check, and the imposition of a protective order, or agreed upon procedures that establish requirements for safeguarding SSI and that are satisfactory to the Secretary of DHS.

(b) Federal employees, contractors, and grantees.

(1) A Federal employee has a "need to know" SSI if access to the information is necessary for performance of the employee’s official duties.

(2) A person acting in the performance of a contract with or grant from DHS has a "need to know" SSI if access to the information is necessary to performance of the contract or grant.

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

4-21
3550 Marking SSI.

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

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

   (2) Any title page; and

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

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

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

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

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

3560 SSI Disclosed by or to the Coast Guard.

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

(b) Disclosure under the Freedom of Information Act and the Privacy Act. If a record contains both SSI and information that is not SSI, the Coast Guard, on a proper Freedom of Information Act or Privacy Act request, may disclose the record with the SSI redacted, provided the record is not otherwise exempt from disclosure under the Freedom of Information Act or Privacy Act.
(c) Disclosures to committees of Congress and the General Accounting Office. Nothing in this part precludes the Coast Guard from disclosing SSI to a committee of Congress authorized to have the information or to the Comptroller General, or to any authorized representative of the Comptroller General.

(d) Disclosure in enforcement proceedings.

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

(2) Obligation to protect information. When an individual receives SSI pursuant to paragraph (d)(1) of this section, that individual becomes a Covered Person under paragraph 3520.1 and is subject to the obligations of a Covered Person under this part.

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

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

3570 Consequences of Unauthorized Disclosure of SSI.

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

3580 Destruction of SSI.

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

(b) Other Covered Persons.

(1) In general. A Covered Person must destroy SSI completely to preclude recognition or reconstruction of the information when the Covered Person no longer needs the SSI to carry out transportation security measures;
(2) Exception. Paragraph (b)(1) of this section does not require a State or local government agency to destroy information that the agency is required to preserve under local law.

3590 Procedures For Communicating SSI Material.

(a) SSI material is to be disseminated to AMS Committee members and/or port stakeholders in accordance with COMDTINST 5510.5:

(1) Hard copy dissemination may be accomplished via:
   i. U.S. Mail;
   ii. interoffice mail; or
   iii. Hand-carrying within/between buildings.

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

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

   (i) Facsimile. The sender must confirm that the facsimile number of the recipient is current and valid and the facsimile machine is in a controlled area where unauthorized persons cannot intercept the SSI facsimile, or the sender must ensure that an authorized recipient is available at the receiving location to promptly retrieve the information. The information to be transmitted must have a cover sheet that clearly identifies the sender’s name and telephone number and contains a warning that, if the message is received by other than the intended recipient, the individual receiving the message must immediately notify the sender for disposition instructions.

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

   (iii) Telephone. The caller must ensure that the person receiving the SSI is an authorized recipient. Individuals needing to pass SSI by telephone will avoid using cellular telephones and cordless telephones unless the circumstances are exigent, or the transmissions are encoded or otherwise protected to reduce the risk of interception and monitoring.
(iv) **Wireless Devices.** The risk of monitoring and interception of SSI is greater when using wireless devices. Therefore, DO NOT use cellular phones, pagers, cordless telephones or personal digital assistants to transmit SSI unless the transmission is encrypted or there is an emergency.

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

3600 Maritime Security Training

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

3700 Security Resources

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

4000 PREVENTION

4100 Introduction

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

4200 Maritime Security (MARSEC) Level Planning

4220 Procedures To Be Used When A Vessel And A Facilities Are At Different MARSEC Levels:

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

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

4230 Procedures For Requesting Equivalencies And Waivers To MARSEC Directives

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

(a) MARSEC Directives will set mandatory measures that all defined entities must meet in a specified time period. These entities will also be required to confirm to the local FMSC receipt of the MARSEC Directive, as well as specify the method by which the mandatory measures have been (or will be) met. Pursuant to 33 CFR 101.130, owners or operators may propose to the local FMSC equivalent security measures that have been approved by Commandant (G-MP) as meeting or exceeding the effectiveness of the required measure.

(b) In addition, 33 CFR §§ 104.130, 105.130, and 106.125 state that vessel or facility owners or operators may request waivers for any requirement of Parts 104, 105, or 106 that the owner or operator considers unnecessary in light of the nature and operating conditions of the vessel or facility. The request must be submitted in writing to Commandant and include justification as to why the specific requirement(s) are unnecessary for that particular owner’s or operator’s vessel or facility or its operating conditions. In the case of facilities regulated under 33 CFR 105, the application must be made prior to operating.

4300 MARSEC Level 1

4310 Roles, Resources, Authorities, and Responsibilities

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

4320 Standard Security Procedures for MARSEC Level 1

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

4330 Physical Security Measures

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

(a) Planning for and establishing Fixed Security Zones and Regulated Navigation Areas (RNAs), and specifying who is going to enforce them;
(b) Incorporating security elements into the duties and responsibilities of all port personnel:

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

c) Establishing restricted areas to control access:

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

(2) Mark restricted areas;

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

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

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

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

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

e) Designating areas where control measures shall be implemented;

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

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

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

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

(j) Offering to review physical security plans and procedures for facilities not regulated under 33 CFR 105 or 106, e.g., electrical transmission lines, communication transmitters, bridges, tunnels, mass transit bridges/tunnels, stadiums, aquariums, amusement parks, waterfront parks, marine events, nuclear power plants, and marinas.

4340 Operational Security (OPSEC) Measures

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

(b) The information about Coast Guard intentions, capabilities, or activities is known as “critical information.” Since the compromise of this critical information may allow a terrorist to gain a significant advantage, its protection involves all personnel, including active duty, reserve, auxiliary, civilian and contractors. A concerted effort must be made to ensure that all personnel are aware that the threat is real and active in all aspects of Coast Guard missions.

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

4400 MARSEC Level 2

4410 Standard Security Procedures for MARSEC Level 2

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

4420 Roles, Resources, Authorities, and Responsibilities

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

4430 Physical Security Measures

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

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

(2) Review of security roles and responsibilities;

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

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

   i. Increase the frequency and detail of monitoring of restricted areas;

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

   iii. Increase control of access points, e.g., assigning additional security personnel;

   iv. Increase detail and frequency of monitoring, including inspection
of individuals, personal effects, and vehicles;

v. Increase frequency of supervised handling of cargo and ship’s stores.

(5) Giving consideration to requiring additional security measures for facilities not regulated under 33 CFR 105 or 106, e.g., electrical transmission lines, communication transmitters, bridges, tunnels, mass transit bridges/tunnels, stadiums, aquariums, amusement parks, waterfront parks, marine events, nuclear power plants, and marinas.

4440 Operational Security Measures

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

4500 MARSEC Level 3

4510 Standard Security Procedures for MARSEC Level 3

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

4520 Roles, Resources, Authorities, and Responsibilities

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

4530 Physical Security Measures

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

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

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

   (1) Monitor restricted areas to protect against an imminent security incident, e.g., secure all access points, prohibit storage of vehicles, cargo and ship’s stores, and maintain continuous patrols;

   (2) Control access, e.g., enhance the security presence at closed access points, provide escorts, and take measures, where practicable, to secure choke points and locations that can be used to observe facility or vessel operations;
(3) Protect against an imminent security incident, e.g., inspect all persons, personal effects and vehicles.

(c) Giving consideration to requiring additional security measures for facilities not regulated under 33 CFR 105 or 106, e.g., electrical transmission lines, communication transmitters, bridges, tunnels, mass transit bridges/tunnels, stadiums, aquariums, amusement parks, waterfront parks, marine events, nuclear power plants, and marinas.

4540 Operational Security Measures

[The AMS Plan will require verification of MARSEC Level 3 OPSEC measures, and may give consideration to requiring additional OPSEC measures for safeguarding information related to vessel arrivals, departures, shiftings and cargoes. Within one hour of receiving reports of MARSEC Level 3 attainment, the FMSC will begin checks of OPSEC measures employed by vessels, and facilities, and vessels and facilities not regulated under 33 CFR 104, 105 and 106, and immediately advise the owner/operator of any violations.]

4600 Public Access Facility

(a) A “Public Access Facility” is an area with public access that is primarily used for recreation or entertainment purposes, and which primary purpose does not include receiving or servicing vessels regulated under 33 CFR 104. This may include a public pier, wharf, dock, waterside restaurant or marina that contains minimal infrastructure, such as only bollards, cleats, or ticket booths. A riverbank that contains no infrastructure may also qualify as a Public Access Facility.

4610 Designation of Public Access Facilities (PAF).

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

(a) An owner or operator may send a written request to the appropriate FMSC requesting to be designated as a PAF in lieu of complying with the requirements of 33 CFR 105. Before granting the exemption, the FMSC shall consider the results of the AMS Assessment. The FMSC will notify the facility in writing whether its request for designation as a PAF has been approved or disapproved.

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

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

Figure 1. Public Access Facility

4620 Withdrawal of Designation

(a) The FMSC may withdraw a facility’s designation as a PAF when the FMSC determines it is necessary. When a designation has been withdrawn from a facility that receives vessels regulated under 33 CFR Part 104, the facility will be required to comply with the requirements of 33 CFR Part 105.

4700 MARITIME WORKER CREDENTIALS (RESERVED)

5000 PREPAREDNESS FOR RESPONSE

5100 Introduction

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

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

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

5110 Procedures for responding to suspicious activity.

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

5120 Procedures for responding to breaches of security.

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

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

5200 Transportation Security Incident (TSI)

5210 Procedures for Notification

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

(a) A TSI will first be reported to the appropriate emergency services to ensure human health and safety measures are taken. Secondary notifications will be made to the FMSC or their representative, then to the NRC.

5220 Incident Command Activation

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

(a) The FMSC, normally in consultation with partner agencies, will determine whether there is a need to establish an incident command or unified command for a particular incident, and what its structure will be.

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

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

5300 Most Probable Transportation Security Incident

(This section will describe the types of TSIIs most likely to occur in the AMS zone, and the procedures and steps that will be taken to respond.)

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

(b) Since it is impossible to plan for every scenario, FMSCs and AMS Committees are directed to plan for a minimum of three scenarios that require exercise of command and control procedures, communications, and the initial response to be taken by port agencies. These plans will be viewed as unofficial Memorandums of Agreement (MOAs) within the port to ensure key players understand what activities each agency will take, and what resources each will bring for the given scenario.

(c) Scenarios should focus on threats and vulnerabilities applicable to that port, such as threats to the common infrastructure, general port threats, and those threats that affect other regulated vessels or facilities. Plans should also focus on several types of scenarios to ensure most port stakeholders are involved in planning efforts. Accordingly, there should be at least one scenario involving a vessel, one for a waterfront facility, and one for a common infrastructure, such as a bridge, tunnel, dam, lock, or other significant structure.

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

5310 Identify Command Structure With Assigned Roles (ICS Flowchart)

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

5320 Procedure For Responding To TSI

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

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

(For each of the three required scenarios, identify what other relevant Federal, State and local plans may be implemented as a result of the
5400 Maritime Security Exercise Requirements

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

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

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

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

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

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

5410 Purpose of Exercise Program

*The AMS Plan will address the frequency and type of exercises it intends to employ in its designated zone.*

(a) The AMS Plan will be tested periodically for currency and efficiency, and to evaluate risk mitigation strategies incorporated into the AMS Plan. Exercise design will be based on threat information and encompass procedures for setting MARSEC Levels. It may be tabletop, field, or a combination of both.

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

5420 Goals of the AMS Plan Exercise Program
(a) The following goals of the Exercise Program should shape the development of exercise scenarios:
   (1) Identification of the performance-based components of the mitigation strategy;
   (2) Gauging the effectiveness of enhanced security measures employed at critical infrastructures within the port area;
   (3) Creating a pool of enhanced adversary characteristics and lessons learned;
   (4) Establishing interaction protocols with other Federal, State and local law enforcement agencies likely to be involved in the overall protection of MTS;
   (5) Updating the exercise-planning guideline.

5430 Exercise Cycle
[The exercise schedule will coordinate with the planning cycle so that information garnered during the exercise can be applied to scheduled revisions to the AMS Plan.]
(a) The AMS Committee is required to execute an exercise once a year with no more than 18 months between exercises. The AMS Committee will develop a 5-year exercise program that details and prioritizes AMS Plan strategies to be analyzed.

5440 Scheduling And Design
(a) The following will be included in designing the exercise program:
   (1) Objectives: Develop exercise goals;
   (2) Concept Development: How will the objectives be attained?
   (3) Scenario and Strategy Selection: Determine the correct strategy and scenario selection to meet exercise objectives;
   (4) Conduct of Exercise: Define how the exercise will meet design objectives and detail scope;
   (5) Control and Evaluation: Detail evaluation and control protocols;
   (6) Data Collection: How will the data be fused?
   (7) After-Action Report: The report will include all aspects of the evaluation process and detail corrective action;
Corrective-Action Plan: How will the corrective action be undertaken? [Detail the methods used to implement change.]

5450 Consideration Of Equivalent Response

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

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

5460 Recordkeeping

(a) Exercise documentation must be retained by the FMSC for 2 years. The AMS Committee Secretary will ensure that all exercise documentation required to be marked as SSI is properly marked and protected from release to the general public.

5470 Linkages Between Family Of Plans Within The Area

[It is envisioned that, in the near future, all area, vessel and facility plans will be digitally stored to provide rapid access to the data during routine and crisis management.]

(a) The following linkages should be considered:

   (1) Vessel and Facility Security Plans;

   (2) State and local plans.

6000 CRISIS MANAGEMENT AND RECOVERY

6100 Introduction

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

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

(b) General priorities for recovery are:

   (1) Major transportation routes needed for emergency services, including evacuation tunnels, bridges, and key waterways;

   (2) Main shipping channels critical for homeland security and homeland defense operations;
(3) Port areas and channels critical for military traffic or out-loads;
(4) Secondary bridges and tunnels;
(5) Main shipping channels critical to major commercial operations;
(6) Secondary commercial waterways;
(7) Public/recreational waterways.

6200 Procedures to Maintain Infrastructure
[The AMS Plan will prioritize infrastructures according to their importance in maintaining the continuity of operations of the port and the procedures for maintaining infrastructure integrity.]

6300 Procedures for Recovery of MTS
[The AMS Plan will prioritize the procedures for most efficient recovery of the MTS and for reopening port(s), and affected waterways, or provide linkages to port plans that address recovery of the MTS.]

7000 COMPLIANCE MEASURES

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

8000 PLAN DOCUMENTATION AND MAINTENANCE

8100 Initial Plan Review and Comment
(a) The FMSC will, after consultation with the AMS Committee, submit an AMS Plan to the appropriate District Commander. The Plan will be submitted on CD ROM and on paper. The appropriate sections of the Plan will be designated SSI.
(b) The District Commanders will conduct the initial AMS Plan review. When conducting the initial review, the District Commander will review each AMS Plan for completeness and content and forward it to the Area Commander who is the approving authority. Upon approval, Area will forward an electronic version of all approved AMS Plans to Commandant G-MP.

8110 Procedures For Continuous Review And Update Of AMS Plans.
[Insert the procedures for review and update of the AMS Plan adopted by the
AMS Committee.

(a) **Informal Review** The update and review of the AMS Plan is an ongoing process. The AMS Committee will review all updates at least annually for accuracy, feasibility, consistency and completeness. The Plan will also be reviewed after each activation, exercise, or drill, and when port conditions change. After each review, the Plan will be updated to include any lessons learned from the activation exercise and drill, and reflect changing port conditions.

(b) **Formal Review** The AMS Committee will conduct a detailed review every 5 years as required by the MTSA. The review will require a re-assessment of the COTP zone covered by the Plan. This will allow for accounting of evolving infrastructure changes.

(c) Portions of the AMS Plan must be updated immediately when certain critical items of information change, including:

1. Emergency points of contact by name and number;
2. SSI eligible recipients and their pertinent verification data;
3. Any changes that alter the communications or notification plan;
4. Any changes in jurisdictional or response capabilities;
5. Any major or minor construction changes that alter avenues of access to facilities.

(d) All updates of the AMS Plan will be submitted to District and Area Commanders as appropriate for review and approval annually, or as substantive changes are made.

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

[Insert procedures for ongoing and annual review of the AMS Assessment.]

(a) The AMS Assessment will also be reviewed and updated to incorporate changes in the port operations and infrastructure. Like the AMS Plan update and review, conducting routine area maritime security assessments is an ongoing process. Accordingly, the assessment should be informally evaluated at least annually for adequacy, feasibility, consistency, completeness and to identify gaps in security.

**9000 APPENDICES (OPTIONAL)**

(a) The AMS Plan contains some information that is intended to reach a broad array of maritime interests while other portions of the AMS Plan will be designated as SSI. As such, some information contained in the Plan is better suited for inclusion in an appendix due to the size or sensitive nature of the information. For example, some information, although not SSI, would be exempt from public disclosure pursuant to 5 USC 553(b).
(b) Examples of appendices are listed below. With the exception of the glossary, the appendices are optional for the development of the AMS Plan.

9100 Area Maritime Security (AMS) Committee Members
[Insert any information tables containing contact and agency names, phone numbers, email addresses, and/or other specific information pertaining to Committee members.]

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

9200 Charts and Maps of Port Areas
[Insert any charts, satellite photographs, maps, or other spatial data defining COTP zone boundaries for a given port.]

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

9300 Port Operations and Infrastructure
[Include portions of the AMS Assessment that list or detail critical port operations and/or infrastructure for a given COTP zone.]

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

9400 Risk-Based Scenarios
[Insert results of the risk-based AMS Assessment pertaining to the identification of threat scenarios specific to a given COTP zone]

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

9500 Dangerous Cargos for Security Planning

9600 Glossary of Terms

(a) A glossary of terms, developed by the Coast Guard Maritime Homeland Security Integration Team, is provided on G-MP intranet site at http://cgweb.comdt.uscg.milig-mp/docs/pdf/PWCS_SDPAp30Sep03.pdf. It was originally developed as an appendix to the Ports, Waterways and Coastal Security (PWCS) Strategy Deployment Plan. The AMS Plan will use the standard terms identified in this glossary.

(b) The following terms are not found in the referenced glossary, but are included as terms used by the DoD and other law enforcement agencies and may be found at http://cgweb.comdt.uscg.mil/g-mp/g-mp.htm
Tab Index

TAB A. Communicating Security Information (Facilities)

TAB B: Communicating Security Information (Commercial Vessels)

TAB C: Security Reports for Suspicious Activity/Security Breach & Quick Response Card Templates

TAB D: SSI Non-Disclosure Agreement
## TAB A: Communicating Security Information (Facilities)

<table>
<thead>
<tr>
<th>Method</th>
<th>Pro's</th>
<th>Con's</th>
<th>Type of info that it can be effective for</th>
</tr>
</thead>
<tbody>
<tr>
<td>NRC notification number</td>
<td>Single point of contact</td>
<td>Designed to report suspicious activities, not security emergencies</td>
<td>Reporting suspicious activity</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Intensive reporting requirement</td>
<td></td>
</tr>
<tr>
<td>911</td>
<td>Readily available in most areas</td>
<td>1-way</td>
<td>Incoming notifications to authorities of suspicious activities or emergencies</td>
</tr>
<tr>
<td></td>
<td>Linkage to translators for multi-lingual calls</td>
<td>Not full coverage</td>
<td></td>
</tr>
<tr>
<td>IAIP (Information Analysis</td>
<td>Targeted to users that need the info</td>
<td>Seems to have a focus on cyber security, however IAIP has expanded their scope to Maritime and Aviation Security</td>
<td></td>
</tr>
<tr>
<td>Infrastructure Protection)</td>
<td>Accepts reports</td>
<td>System overload</td>
<td></td>
</tr>
<tr>
<td>Port Security Facility Officer</td>
<td>Existing, recognized system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>under ISPS Code (MTSA designated USCG COTP as this)</td>
<td>Tested system</td>
<td></td>
<td></td>
</tr>
<tr>
<td>Qualified Individual (QI)</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>US ACOE Lockmaster</td>
<td>Back-up if other systems fail – communicate to Lockmaster at next lock</td>
<td>Limited availability – only where locks exist</td>
<td></td>
</tr>
<tr>
<td>Use of code words (both positive and negative code words)</td>
<td>Secure</td>
<td>Not used everywhere</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Minimal cost</td>
<td>Requires training and awareness</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can be used under duress in many cases</td>
<td>Security could be compromised</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can be used onboard vessel for crew, or to dialog back to home office or to agencies (i.e. pilots to VTS)</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
## TAB B: Communicating Security Information (Commercial Vessels)

<table>
<thead>
<tr>
<th>Method</th>
<th>Pro’s</th>
<th>Con’s</th>
<th>Type of info that it can be effective for</th>
</tr>
</thead>
<tbody>
<tr>
<td>GMDDSS</td>
<td>Very regional, so can provide specific info</td>
<td>Deep-sea only 1-way comms only (vessel receives info, but can’t send)</td>
<td>Communicating info to ships entering US waters</td>
</tr>
<tr>
<td>NAVTEX</td>
<td>Mass distribution</td>
<td>Have to have a computer</td>
<td>General security information</td>
</tr>
<tr>
<td></td>
<td>Reliably</td>
<td>Keeping e-mail addresses updated</td>
<td>Can be used to communicate threat levels and other info (must be supplemented by other means due to passive issue)</td>
</tr>
<tr>
<td></td>
<td>Handles lots of info</td>
<td>Not necessarily immediate</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2-way comms</td>
<td>Passive – you usually have to look for it</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Might not be secure</td>
<td></td>
</tr>
<tr>
<td>E-mail</td>
<td>Provides world-wide geographic position of vessels</td>
<td>Normally 1-way comms only (vessel to system)</td>
<td>Can be used to identify position of ships</td>
</tr>
<tr>
<td></td>
<td>Can be used 2-way</td>
<td>Voluntary</td>
<td>Can be used to provide ANOA’s</td>
</tr>
<tr>
<td>AMVER</td>
<td>Reliable</td>
<td>Can be blocked in some areas by topography</td>
<td>Can be used for just about anything as long as it is working. In data format, can be used for broad distribution</td>
</tr>
<tr>
<td></td>
<td>Transmission secure</td>
<td>Not redundant – a system goes down, you might lose coverage</td>
<td></td>
</tr>
<tr>
<td>Satellite (voice and data)</td>
<td>Widespread availability of geographic position of vessels</td>
<td>Can be used 2-way</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Reliable</td>
<td>Voluntary</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Transmission secure</td>
<td>Can be used for just about anything as long as it is working. In data format, can be used for broad distribution</td>
<td></td>
</tr>
<tr>
<td>VHF</td>
<td>Widespread availability of geographic position of vessels</td>
<td>Short range – line of sight, although repeaters can be used</td>
<td>Can communicate any info needed, provided not SSI</td>
</tr>
<tr>
<td></td>
<td>Immediately available</td>
<td>Not secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td>2-way comms</td>
<td>Not guaranteed delivery - Not everyone has it or monitors it at all times</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Economical</td>
<td>Relies on someone recording what they hear over the VHF</td>
<td></td>
</tr>
<tr>
<td>UHF</td>
<td>Often used for search and rescue and/or emergency response</td>
<td>Longer range than VHF, but range can be limited – repeaters can be used to extend range</td>
<td>Same as VHS</td>
</tr>
<tr>
<td></td>
<td>Widespread availability of geographic position of vessels</td>
<td>Limited pool/availability of users</td>
<td></td>
</tr>
<tr>
<td>RACES (HAM operated system)</td>
<td>Long range</td>
<td>Not secure</td>
<td>Back-up communications system</td>
</tr>
<tr>
<td></td>
<td>Reliable (will operate)</td>
<td>Limited resources</td>
<td>Not a primary system for communicating threats</td>
</tr>
<tr>
<td></td>
<td>System has to be activated</td>
<td>System has to be activated</td>
<td></td>
</tr>
<tr>
<td>EPIRB</td>
<td>Self-activating system “after the fact”</td>
<td>Used for distress and providing location, but does not provide the cause of the problem</td>
<td>Could alert authorities that a vessel is in distress (responders need to be aware that it could now be a security issue)</td>
</tr>
<tr>
<td></td>
<td>Provides location</td>
<td>One-way only</td>
<td></td>
</tr>
<tr>
<td>Cellular</td>
<td>Widespread availability of geographic position of vessels</td>
<td>Limited range</td>
<td>Can be used with computers</td>
</tr>
<tr>
<td></td>
<td>Inexpensive</td>
<td>Not reliable</td>
<td>One of most effective ways to communicate immediate changes</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Not secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>System prone to overload</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Can’t be used for mass communications (conf Calls)</td>
<td></td>
</tr>
<tr>
<td>Pagers</td>
<td>Widespread availability of geographic position of vessels</td>
<td>May not be 100% coverage</td>
<td>Short informational bulletins</td>
</tr>
<tr>
<td></td>
<td>Inexpensive</td>
<td>Not necessarily reliable</td>
<td>Must be supplemented by other means to insure notification</td>
</tr>
<tr>
<td></td>
<td>Can be 2-way and guaranteed delivery</td>
<td>Not secure</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Messages can be delayed</td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
<td>Land-based system</td>
<td></td>
</tr>
<tr>
<td>Landline (telephone)</td>
<td>Widespread availability in buildings</td>
<td>Not available on vessels</td>
<td>Anything, but may need to be supplemented by other means if not successful</td>
</tr>
<tr>
<td></td>
<td>Generally reliable</td>
<td>Can be overloaded</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Can be made secure</td>
<td>Person being called may not be in to receive call/message</td>
<td></td>
</tr>
</tbody>
</table>
| **Fax** | Widely available  
Generally reliable  
Can be made secure  
Can broadcast fax | Can be overloaded  
No guarantee fax is picked-up by someone | Anything, but may need to be supplemented by other means  
Particular effective for broadcast fax  
Robust systems exist with additional options |
| --- | --- | --- | --- |
| **Internet web sites** | Easily accessible  
Can be made secure  
Can share large amounts of information | May be difficult to manage access  
Passive - Have to know to go look | Can be used to verify current threat level  
Can be used for general interest info (non-SSI)  
Can provide greater detail once stakeholders informed to go look |
| **AIS** | Great navigational tool for vessels and VTS  
Can be used to identify location of vessels in the area | Can be used by terrorists if they get the equipment  
Local system with limited range  
Have to have the equipment to use it - costly  
Some of same limitations of VHS | A navigational tool that enhances Maritime Domain Awareness, allows for the efficient exchange of vessel traffic information |
| **Navigational aids (lights, buoys, etc.)** | Readily visible for a local area  
May be used to designate security zones, RNA’s, etc. | Not every waterway user understands what they mean  
Upkeep and maintenance  
Slow deployment process  
Can be affected by waterway conditions (high or low water/flow) | Can be used to designate security zones, RNA’s, etc. |
| **IRRIS** | Highly integrated system  
Secure system  
May be possible to integrate with some existing systems that companies use | Has to be developed for non-gov’t use  
No req’t to use today | May be an option to AIS for certain applications  
Integrates data from many sources  
Good response and planning tool |
| **First Mate, produced by GENMAR** | Essentially “On Star” for marine vessels – provides similar functionality  
Relatively new, but not overly expensive | Developed for US recreational use only  
May have similar limitations to satellite | May be used for security, tracking, and notification of boats in an affected area  
May be an effective tool for reporting an emergency  
Need to outreach to the company so that they know who to notify |
| **EAS (Emergency Alert System) and TV/Radio broadcast systems** | Wide dissemination of info  
Recognized system for the public  
Widely available | No guarantee of delivery since people may not be monitoring TV/radio  
Land-based, limited area of delivery  
Not for SSI info | Can be used to alert local areas for emergency notifications |
| **Local area systems (CAN – Community alert networks, Reverse 911, sirens, CAER systems, etc.)** | Provides saturated, local, targeted coverage  
Can identify who has been notified, but not that they understood the message | Very localized  
Subject to system failures  
Not available everywhere  
Have to answer phone to receive message  
Do “zappers” defeat the incoming calls? | Can be used to alert local areas for emergency notifications |
| **US ACOE system for communicating between locks** | Very fast and effective system  
Standalone hard-wired radio repeater system (VHF and UHF) | Limited access  
If other systems down, have to get to ACOE system (physically go there) to communicate  
System life in question  
Similar “cons” as listed for UHF/VHF communications) | Back-up communications for USCG and others during an emergency |
| **WATERCOM – Waterways communication system by MOBEX** | Existing system  
Covers about 90% of inland waterways | Short life remaining (may be shut down within 5 years)  
Limited area of coverage  
Expensive | Use to communicate with vessels that have the equipment installed |
| Marine Exchange (clearinghouse for marine information) | Central comms clearinghouse between gov't and industry | Not in all ports Not-for-profit, so has to be a cooperative effort to use it Voluntary use | Communicate between agents, vessel owners, operators, facility owners, port authorities, etc. |
| Secure VCT for DHS to state Emergency Management directors | Secure phone/fax between DHS and state EM directors | In developmental stages Limited access to info Not sure how EM directors will route info down to industry | Can be used to disseminate info to state officials State officials could disseminate further |
| Secure gov't comms. | Secure Limited access | Limited access Not available to industry | Secondary and tertiary comms networks if local networks/systems fail |
| Trunked Systems | Moderately secure Can patch system to VHF/UHF (additional cost) | Not everyone uses the same systems Relatively short range Systems can get overloaded Probably can't be used to call 911 | Similar to VHF, but with limited/restricted accessibility |
| Amber Alert System | Public system Fast and efficient Thorough | Can't assure who received it (passive) Never been used for security Limited resources in rural areas Need to identify trigger One way | Can be used to communicate threat levels, non-SSI info Communicate info in an emergency |
| NOAA Tone Alert (Weather Radio) | Wide availability System is readily expandable | Passive system 1-way Not everyone has receivers Never used for security before Limited audience | Can be used to communicate threat levels, non-SSI info Communicate info in an emergency |
**SUSPICIOUS ACTIVITY**

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

<table>
<thead>
<tr>
<th><strong>INITIAL INFORMATION</strong></th>
<th><strong>Date/Time of Report</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>OOD</strong></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Reporting Party</strong></th>
<th><strong>Phone</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Location</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>VESSEL INFORMATION:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Vessel</strong></td>
</tr>
<tr>
<td>------------</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Lloyds Number</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Gross Tons</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Cargo Type</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Lat</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Course/Speed</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Port of Origin</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>ETA</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>Owner</strong></th>
<th><strong>Phone</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Agent</strong></td>
<td><strong>Phone</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Fax</strong></td>
<td></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Other</strong></td>
<td><strong>information</strong></td>
</tr>
<tr>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th><strong>FACILITY INFORMATION:</strong></th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Facility</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>Location</strong></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td><strong>POC</strong></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>
TAB C

Phone __________________________ __
Other information

OTHER INFORMATION:
Agencies on scene________________________ USCG resources on scene________________________

DESCRIPTION OF SITUATION:

SUSPICIOUS ACTIVITY (cont)

ACTION CHECKLIST

<table>
<thead>
<tr>
<th>Arrange:</th>
<th>YES</th>
<th>NO</th>
<th>TIME/DATE</th>
<th>OTHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>FOSC</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Firefighting</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Underway:</th>
<th>YES</th>
<th>NO</th>
<th>TIME/DATE</th>
<th>OTHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Boat</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Helo</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Dispatch/Notify:</th>
<th>YES</th>
<th>NO</th>
<th>TIME/DATE</th>
<th>OTHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Recall Team</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MER</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Port Safety</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duty Inspector</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Duty Invest.</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSD</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Establish</th>
<th>YES</th>
<th>NO</th>
<th>TIME/DATE</th>
<th>OTHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>Safety Zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Security Zone</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>COTP Order</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Custom's Hold</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Restricted Airspace</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>Notify:</th>
<th>YES</th>
<th>NO</th>
<th>TIME/DATE</th>
<th>OTHER</th>
</tr>
</thead>
<tbody>
<tr>
<td>CDO /CPOPS/XO/CO</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>VTS</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>District</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>GROUP OPCEN</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>MSGD</td>
<td>Sheriff</td>
<td>Police</td>
<td>U.S. Marshal</td>
<td>FBI</td>
</tr>
<tr>
<td>-----------</td>
<td>---------</td>
<td>--------</td>
<td>--------------</td>
<td>-----</td>
</tr>
</tbody>
</table>

**Messages:**
- SITREP/POLREP
- BNTM
- Req. Resources

**Case Info:**
- Statements
- Photos

Other action taken
**TERRORISM/HOSTAGE SITUATION**

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

<table>
<thead>
<tr>
<th>INITIAL INFORMATION</th>
<th>Date/Time of Report__________________________</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OOD___________________________________________</td>
</tr>
</tbody>
</table>

Notified by__________________________________________
Phone__________________________________________

**TERRORIST/HOSTAGE INFORMATION:**

Number of Terrorists/Hostages__________________________
Nationality________________________________________

Number of Hostage Takers__________________________
Nationality________________________________________

Name(s)__________________________________________

Age(s)__________________________________________

Health Conditions________________________________

Weapons__________________________________________

Terrorist activity/Demands__________________________

Location__________________________________________

**VESSEL/FACILITY INFORMATION:**

Vessel/Facility__________________________ Vessel/Facility Type__________________________
Lat__________________________ Long__________________________
Course/Speed__________________________
Port of Origin__________________________
Destination__________________________
OTHER INFORMATION:

Agencies on scene __________________________ USCG Resources on scene __________________________

Communications ____________________________

Other Comments ____________________________

TERRORISM/HOSTAGE SITUATION (cont.)

ACTION CHECKLIST
(Time) (Person Notified)

___ Notify CDO

___ Notify District Command Center

___ Notify State and Local Enforcement Agencies

___ Notify FBI (###)-###-####

___ What assistance is necessary to support the FBI?

___ Emergency Safety Zone

___ Small boat assistance for transport of FBI or as weapons platform. <Action Groups>

___ Small boat assistance in evacuating personnel. <Action Group NOLA>

___ Notify VTS when applicable

ADDITIONAL REFERENCES:

BOMB THREAT - Vessel or Facility

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

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

<table>
<thead>
<tr>
<th>INITIAL INFORMATION</th>
<th>Date/Time of Report __________________</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>OOD _________________________________</td>
</tr>
</tbody>
</table>

What does it look like?

Exact words of person calling:

Name of Threatened Vessel/Facility ________________________________

Name of Owner/Operator ________________________________

Phone ________________________________

Address of Facility/Location of Vessel ________________________________

QUESTIONS TO ASK

When is it set to go off? ________________________________ (unknown)

Where is it? ________________________________ (unknown)

What kind of bomb is it? ________________________________ (unknown)

Why did you place the bomb? ________________________________ (unknown)

Who (what organization) is responsible? ________________________________ (unknown)

DESCRIPTION OF CALLER’S VOICE

Male/Female ____________________________________________ Age ________________________________

Intoxicated ________________________________ Speech Impediment ________________________________

Accent ________________________________
### Scripted - Ad Lib

**Recorded**

### BACKGROUND NOISES:

<table>
<thead>
<tr>
<th>Music</th>
<th>Children</th>
</tr>
</thead>
<tbody>
<tr>
<td>Airplane</td>
<td></td>
</tr>
<tr>
<td>Talk</td>
<td>Traffic</td>
</tr>
<tr>
<td>Typing</td>
<td></td>
</tr>
<tr>
<td>Machines</td>
<td>Boating</td>
</tr>
<tr>
<td>Fan/Vent</td>
<td>Other</td>
</tr>
</tbody>
</table>

### BOMB THREAT - Vessel/Facility (cont.)

#### ACTION CHECKLIST

**Time**

- **Notify** the Vessel agent/operating company and/or Facility **IMMEDIATELY** *(If not already aware)*
  - **Inform** them **NOT** to use radios or cell phones. **Recommend** they evacuate all personnel
- **Notify** CDO
- **Notify** State Police Bomb Squad (###) ###-####
- **Notify** FBI (N.O. Branch) (###) ###-####
- **Notify** Police Dept. and Fire Dept. via 911
- **Notify** VTS *(Consider waterway and traffic issues)*
- **Notify** District Command Center and Group NOLA

- Find what assistance, if any, are the Police requesting from the USCG
- Determine if emergency Safety Zone is necessary.
- Determine if small boat assistance in transporting Bomb Squads to vessel *(CG Group)* is necessary.
- Determine if small boat assistance in evacuating personnel *(CG Group)* is necessary.

#### ADDITIONAL REFERENCES:

(a) 33 CFR 6.19  
(b) Marine Safety Manual, Vol. VII *(Chapter 6)*  
(c) CGD_SOP  
(d) Physical Security Manual, COMDTINST M5530.1
I, ______________________ hereby consent to the terms in this Agreement in consideration of my being granted conditional access to certain United States Government documents or material containing sensitive but unclassified information.

I understand and agree to the following terms and conditions:

1. By being granted conditional access to sensitive but unclassified information, the United States Government has placed special confidence and trust in me and I am obligated to protect this information from unauthorized disclosure, in accordance with the terms of this Agreement.

2. As used in this Agreement, sensitive but unclassified information is any information which the loss of, misuse of, or unauthorized access to or modification of could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under Title 5, U.S.C., Section 552a, but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

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

4. I will never divulge any sensitive but unclassified information that is provided to me pursuant to this Agreement to anyone unless I have been advised in writing by the Department of Homeland Security that the individual is authorized to receive it. Should I desire to make use of any sensitive but unclassified information, I will do so in accordance with paragraph 6 of this Agreement. I will submit to the Department of Homeland Security for security review, prior to any submission for publication, any book, article, column or other written work for general publication that is based upon any knowledge I obtained during the course of my work on (identify) in order for the Dept. of Homeland Security to ensure that no sensitive but unclassified information is disclosed.

5. I hereby assign to the United States Government all royalties, remunerations, and emoluments that have resulted, will result, or may result from any disclosure, publication, or revelation of sensitive but unclassified information not consistent with the terms of this Agreement.

6. I hereby agree that when reviewing any official documents containing sensitive but unclassified information, such review will be conducted at a secure facility or under circumstances that will maintain the security protection of such material. I will not be permitted to and will not make any copies of documents or parts of documents to which conditional access is granted to me. Any notes taken during the course of such access will remain at the Department of Homeland Security, to be placed in secure storage unless it is determined by the Department of Homeland Security that the notes contain no sensitive but unclassified information. If I wish to have the notes released to me, Department of Homeland Security officials will review the notes for the purposes of deleting any sensitive but unclassified information to create a redacted copy of the notes. If I do not wish a review of any notes that I make, those notes will remain sealed in secure storage at the Department of Homeland Security.

7. If I violate the terms and conditions of this Agreement, I understand that the unauthorized disclosure of sensitive but unclassified information could compromise the security to the Department of Homeland Security.
8. If I violate the terms and conditions of this Agreement, such violation may result in the cancellation of my conditional access to sensitive but unclassified information. This may serve as a basis for denying me conditional access to Department of Homeland Security information, both classified and sensitive but unclassified information in the future. If I violate the terms and conditions of this Agreement, the United States may institute a civil action for damages or any other appropriate relief. The willful disclosure of information to which I have agreed therein not to divulge may constitute a criminal offense.

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

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

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

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

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

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

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

________________________________________  ______________________________
DATE NAME (Last, First, Middle I.)

This Agreement was accepted by the undersigned on behalf of the Department of Homeland Security as a prior condition of conditional access to sensitive but unclassified information.

________________________________________  ______________________________
DATE WITNESSED BY - Department of Homeland Security

U.S. DEPARTMENT OF HOMELAND SECURITY HSIF 4024 (01/2003)

This form is not subject to the requirements of P. L. 104-13, "Paperwork Reduction Act of 1995" 44 USC, Chapter 35.
PORT SECURITY ASSESSMENT

BACKGROUND.

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

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

\[ R = P \times C \]

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

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

DISCUSSION.

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

A criticality assessment is a process designed to systematically identify and evaluate important assets and infrastructure in terms of various factors, such as the mission and significance of a target. For example, nuclear power plants, key bridges, and major computer networks might be identified as “critical” in terms of their importance to public safety, national security, and economic activity. In addition, facilities might be critical at certain times, but not others. For example, large sports stadiums, shopping malls, or office towers may represent an important target only when in use by large numbers of people. Criticality assessments are important
because they provide a basis for focusing the mitigation strategies and implementation methods on the most important items by identifying which assets and structures are more crucial to protect from an attack. Criticality assessments consider such factors as the importance of a structure to the missions of the port, the ability to reconstitute this capability, and the potential cost to repair or replace the asset. Criticality assessments should also give information on impacts to life, economic security, symbolic value and national defense. Criticality assessments provide information to prioritize assets and determine which potential targets merit further evaluation.

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

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

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

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

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

The overall steps of this security assessment are -

1. Perform a criticality assessment to identify critical activities or operations. This will lead to the identification of critical targets with the port. Table 1 provides an example for performing a criticality assessment of the targets. A blank worksheet is provided at the end of this enclosure.

2. Conduct a threat assessment to define scenarios by combining threats with credible attack scenarios. Table 2 lists some possible scenarios.

3. Conduct consequence and vulnerability assessments for each target/scenario combination using a high, medium, low score based on descriptors of specific elements in Tables 3 and 4. Table 3 lists several consequence elements to consider and Table 4 lists several vulnerability elements to consider. Note that consensus should be reached on a single overall consequence score and a single overall vulnerability score for each target/scenario combination.

4. Categorize the target/scenario combinations using Table 5. Table 5 prioritizes scenarios by organizing them into three categories: those for which mitigation strategies should be developed; those that should be considered on a case-by-case basis; and those that do not need mitigation strategies and need only to be documented.

5. Determine mitigation strategies and implementation methods using Tables 6 and 7. Strategies and methods need to consider the varying degrees of security threat (i.e., MARSEC levels).

An expanded explanation of the steps follows:

**STEP 1: CRITICALITY ASSESSMENT**

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

Identify those specific infrastructure targets that support critical operations of the port. All identified targets should be included in the evaluation. Targets considered, but dismissed for evaluation should be documented for future reference. While not all encompassing, the following table lists general classes of targets that should be considered. In addition, it is important to consider the role or mission of the target in the operation of the port. Broadly, we consider five mission or operation areas to be of interest. These are Public Health, Commerce, Safety/Defense, Transportation and Communications. The effect of destruction considers which consequence factors are affected by the loss of the target. The next consideration in determining
Criticality is the ability to recover from destruction of the target. If an individual bridge is considered, but it is one of four parallel bridges crossing the same waterway, the ability of the port to recover from its destruction is likely to be better than if it is the only means. Finally, consider the number of mission areas affected, the degree of the effects and the ability to recover and make an overall assessment of the criticality.

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

Table 1: Criticality Assessment

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

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

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

STEP 2: THREAT ASSESSMENT AND SCENARIO SELECTION

An attack scenario consists of a potential threat to a unique target or target class under specific circumstances. It is important that the developed scenario or scenarios are within the realm of possibility and, at a minimum, address known capabilities and intents as evidenced by past events and available intelligence. For example, a boat containing explosives (a specific class of scenario) ramming a tanker (target) that is outbound through a choke point (specific circumstance) is one credible scenario. It is much less credible that a U.S. Navy ship will be
commandeered and used to ram a bridge unless specific intelligence reports indicate otherwise. Table 2 provides a notional list of scenarios that may be combined with specific critical targets to develop the scenarios to be evaluated in the Port Security Assessment.

Table 2: Notional List of Scenarios

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

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

**STEP 3: CONDUCTING A CONSEQUENCE AND VULNERABILITY ASSESSMENT**

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

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

**Table 3: Consequence Categories**

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

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

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

**Table 4: Consequence Score**

5-6
Four elements of vulnerability are included in the computation of the vulnerability score: availability, accessibility, organic security, and target hardness. A descriptor of the vulnerability components follows in Table 5.

**Table 5: Vulnerability Categories**

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

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

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

STEP 4: CATEGORIZING THE TARGET/SCENARIO COMBINATIONS

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

Table 7. Vulnerability & Consequence Matrix

<table>
<thead>
<tr>
<th>Vulnerability Score</th>
<th>Low</th>
<th>Medium</th>
<th>High</th>
</tr>
</thead>
<tbody>
<tr>
<td>Consequence Score</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>High</td>
<td>Consider</td>
<td>Mitigate</td>
<td>Mitigate</td>
</tr>
<tr>
<td>Medium</td>
<td>Document</td>
<td>Consider</td>
<td>Mitigate</td>
</tr>
<tr>
<td>Low</td>
<td>Document</td>
<td>Document</td>
<td>Document</td>
</tr>
</tbody>
</table>

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

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

**STEP 5: DETERMINING MITIGATION STRATEGIES AND IMPLEMENTATION METHODS**

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

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

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

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

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

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

A strategy may be thought of as effective if its implementation lowers the overall consequence or vulnerability score. A strategy may be thought of as partially effective if the strategy will lower an overall score when implemented along with one or more other strategies. A strategy may be thought of as having no effect if its implementation does not lower a score.
A strategy may be thought of as feasible if it can be implemented with little trouble or funding within current budgetary constraints. A strategy may be thought of as partially feasible if its implementation requires significant changes or additional funding. A strategy may be thought of as not feasible if its implementation is problematic or is cost prohibitive except under extreme threat conditions.

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

After the selection of the mitigation strategies and implementation methods, the PSC should check the results to ensure that critical operations are maintained and the risk is reduced to the port. Some mitigation strategies might include shutting down non-critical operations during higher threats.
### Table 9: Mitigation Strategy Development Worksheet – EXAMPLE

<table>
<thead>
<tr>
<th>Target: Cruise Liner Scenario: Intentional Sinking</th>
<th>Mitigation Strategy</th>
<th>Strategy Reduces:</th>
<th>Vulnerability</th>
<th>Consequence</th>
</tr>
</thead>
<tbody>
<tr>
<td>Intentional sinking of cruise vessel while embarking/disembarking passengers</td>
<td>Requires vessel to post lookouts while moored.</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Receives and communicates emergent threat information</td>
<td>X X</td>
<td>X</td>
<td></td>
</tr>
<tr>
<td></td>
<td>Requires small boat patrol on waterside</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Has identified adequate medical &amp; law enforcement response personnel in case of attack</td>
<td>X</td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Restricts non-essential personnel from area close to passenger terminal</td>
<td>X</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

### Table 10: Mitigation Strategy Benefit Analysis – EXAMPLE

<table>
<thead>
<tr>
<th>Target: Cruise Liner</th>
<th>Scenario: Intentional Sinking</th>
<th>Effective</th>
<th>Feasible</th>
<th>Apply in threat level:</th>
<th>Resources</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strategy</td>
<td>Yes/Partially/No</td>
<td>Yes/Partially/No</td>
<td>Low/Med/High/None</td>
<td>Available/Gap</td>
<td></td>
</tr>
<tr>
<td>Armed lookouts</td>
<td>Yes</td>
<td>Yes</td>
<td>x</td>
<td>x</td>
<td>x</td>
</tr>
<tr>
<td>Emergent threat information</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Small boat patrol</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Adequate response personnel</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
<tr>
<td>Restrict non-essential personnel</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td>x</td>
<td></td>
</tr>
</tbody>
</table>
## Port Security Assessment

<table>
<thead>
<tr>
<th>Target</th>
<th>Scenario</th>
<th>Criticality</th>
<th>Consequence</th>
<th>Vulnerability</th>
<th>Action</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td></td>
<td>Critical, Moderate, Marginal</td>
<td>High, Medium, Low</td>
<td>High, Medium, Low</td>
<td>Mitigate, Consider Document</td>
</tr>
</tbody>
</table>