(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."

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 1 has been set;

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

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

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

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

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

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

4340 Operational Security (OPSEC) Measures

(a) Operational Security is defined as a systematic and analytical process by

which the U.S. Government and its supporting contractors can deny potential adversaries information about capabilities and intentions by identifying, controlling, and protecting evidence of planning and execution of sensitive activities and operations.

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

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

4400 MARSEC Level 2

4410 Standard Security Procedures for MARSEC Level 2

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

4420 Roles, Resources, Authorities, and Responsibilities

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

4430 Physical Security Measures

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

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

(2) Review of security roles and responsibilities;

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

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

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

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

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

iv. Increase detail and frequency of monitoring, including inspection

of individuals, personal effects, and vehicles;

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

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

4440 Operational Security Measures

[The AMS Plan shall detail procedures to verify attainment of MARSEC Level 2 OPSEC measures, and may give consideration to requiring additional OPSEC measures for safeguarding information related to vessel arrivals, departure, shiftngs, and cargoes. Within four hours of receiving reports of MARSEC 2 attainment, 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.]

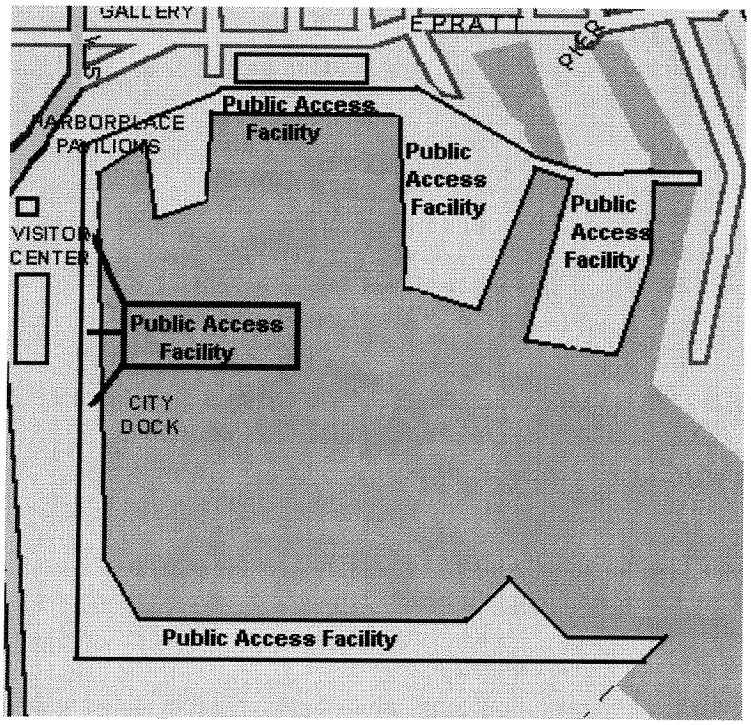
(a) An owner or operator may send a written request to the appropriate FMSC requesting to be designated as a PAF in lieu of complying with the requirements of 33 CFR 105. Before granting the exemption, the FMSC shall consider the results of the AMS Assessment. The FMSC will notify the facility in writing 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 TSIs most likely to occur in the AMS zone, and the procedures and steps that will be taken to respond.]

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

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

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

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

5310 Identify Command Structure With Assigned Roles (ICS Flowchart)

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

5320 Procedure For Responding To TSI

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

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

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

scenario.]

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;

(8) 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 on-going 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.mil/g-mp/docs/pdf/PWCS_SDP_AppA_30Sep03.pdf . It was originally developed as an appendix to the Ports, Waterways and Coastal Security (PWCS) Strategy Deployment Plan. The AMS Plan will use the standard terms identified in this glossary.

(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)

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

TAB B: Communicating Security Information (Commercial Vessels)

Method	Pro's	Con's	Type of info that it can be effective for
GMDSS			
NAVTEX	Very regional, so can provide specific info	Deep-sea only 1-way comms only (vessel receives info, but can't send) Cannot be used for SSI info	Communicating info to ships entering US waters
E-mail	Mass distribution Reliable Handles lots of info 2-way comms	Have to have a computer Keeping e-mail addresses updated Not necessarily immediate Passive – you usually have to look for it Might not be secure	General security information Can be used to communicate threat levels and other info (must be supplemented by other methods due to passive issue)
AMVER	Provides world-wide geographic position of vessels Can be used 2-way	Normally 1-way comms only (vessel to system) Voluntary	Can be used to identify position of ships Can be used to provide ANOA's
Satellite (voice and data)	Reliable Transmission secure	Can be blocked in some areas by topography Not redundant – a system goes down, you might lose coverage Expensive	Can be used for just about anything as long as it is working. In data format, can be used for broad distribution
VHF	Widely available Immediately available 2-way Economical	Short range – line of sight, although repeaters can be used Not secure Not guaranteed delivery - Not everyone has it or monitors it at all times Relies on someone recording what they hear over the VHF	Can communicate any info needed, provided not SSI
UHF	Often used for search and rescue and/or emergency response	Longer range than VHF, but range can be limited – repeaters can be used to extend range Limited pool/availability of users	Same as VHS
RACES (HAM operated system)	Long range Reliable (will operate)	Not secure Limited resources System has to be activated	Back-up communications system Not a primary system for communicating threats
EPIRB	Self-activating system "after the fact" Provides location	Used for distress and providing location, but does not provide the cause of the problem One-way only	Could alert authorities that a vessel is in distress (responders need to be aware that it could now be a security issue)
Cellular	Widely available Inexpensive	Limited range Not reliable Not secure System prone to overload Can't be used for mass communications (conf. Calls)	Can be used with computers One of most effective ways to communicate immediate changes
Pagers	Widely available Inexpensive Can be 2-way and guaranteed delivery	May not be 100% coverage Not necessarily reliable Not secure Messages can be delayed Land-based system	Short informational bulletins Must be supplemented by other means to insure notification
Landline (telephone)	Widely available in buildings Generally reliable Can be made secure	Not available on vessels Can be overloaded Person being called may not be in to receive call/message	Anything, but may need to be supplemented by other means if not successful

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	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

TAB C

SUSPICIOUS ACTIVITY

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

INITIAL INFORMATION Date/Time of Report_____
OOD_____

Reporting Party_____
Phone_____

Location_____
___

VESSEL INFORMATION:

Vessel_____ Vessel
Type_____

Lloyds Number_____
Homeport_____

Gross Tons_____ Deadweight Tons_____ Prop
Type_____

Cargo Type_____
Amount_____

Lat_____ Long_____
Course/Speed_____

Port of Origin_____ Destination_____
ETA_____

Owner_____
Phone_____

Agent _____ Phone_____
Fax_____

Other
information_____

_____
____

FACILITY INFORMATION:

Facility_____
Location_____

POC_____

Phone_____

Other information_____

_____

_____

OTHER INFORMATION:

Agencies on scene_____ USCG resources on scene_____

DESCRIPTION OF SITUATION:

_____

_____

_____

_____

_____

_____

SUSPICIOUS ACTIVITY (cont)

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

TAB C

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

Other action taken_____

_____

_____

TAB C

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.

INITIAL INFORMATION Date/Time of Report_____
OOD_____

Notified by_____
Phone_____

TERRORIST/HOSTAGE INFORMATION:

Number of Terrorists/Hostages_____
Nationality_____

Number of Hostage Takers_____
Nationality_____

Name(s)_____
_____

Age(s)_____
_____

Health
Conditions_____

Weapons
_____

Terrorist
activity/Demands_____

_____
_____

Location_____
_____

_____
_____

VESSEL/FACILITY INFORMATION:

Vessel/Facility_____ Vessel/Facility
Type_____

Lat_____ Long_____
Course/Speed_____

Port of Origin_____
Destination_____

OTHER INFORMATION:

Agencies on scene_____USCG Resources on scene_____

Communications_____

Other Comments_____

TERRORISM/HOSTAGE SITUATION (cont.)

ACTION CHECKLIST

(Time) (Person Notified)

____ Notify CDO
____ Notify District Command Center _____
____ Notify State and Local Enforcement Agencies
_____
____ Notify FBI (###)-###-#### _____
____ What assistance is necessary to support the FBI?
    ____ Emergency Safety Zone
    ____ Small boat assistance for transport of FBI or as weapons platform. <Action Groups>
    ____ Small boat assistance in evacuating personnel. <Action Group NOLA>
____ Notify VTS when applicable

ADDITIONAL REFERENCES:

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

TAB C

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 <u>Don't Hang Up!!</u>

INITIAL INFORMATION Date/Time of Report_____
OOD_____

What does it look like?

_____

Exact words of person
calling:_____

Name of Threatened
Vessel/Facility_____

Name of Owner/Operator_____
Phone_____

Address of Facility/Location of
Vessel_____

QUESTIONS TO ASK

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

Where is it? _____
(unknown)

What kind of bomb is it? _____
(unknown)

Why did you place the bomb? _____
(unknown)

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

DESCRIPTION OF CALLER'S VOICE

Male/Female_____ Age_____

Intoxicated_____ Speech Impediment_____
Accent_____

Scripted_____ Ad Lib_____
Recorded_____

BACKGROUND NOISES:

Music_____ Children_____
Airplane_____

Talk_____ Traffic_____
Typing_____

Machines_____ Boating_____
Fan/Vent_____ Other_____

BOMB THREAT - Vessel/Facility(cont.)

ACTION CHECKLIST
(Time)

____ Notify the Vessel agent/operating company and/or Facility **IMMEDIATELY** (If not already aware)
Inform them NOT to use radios or cell phones. Recommend they evacuate all personnel
____ Notify CDO
____ Notify State Police Bomb Squad (###) ###-#### _____
____ Notify FBI (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 is small boat assistance in evacuating personnel (CG Group) is necessary.

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

CONDITIONAL ACCESS TO SENSITIVE BUT UNCLASSIFIED INFORMATION NON-DISCLOSURE AGREEMENT

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

I understand and agree to the following terms and conditions:

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

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

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

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

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

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

7. If I violate the terms and conditions of this Agreement, I understand that the unauthorized disclosure of sensitive but unclassified information could compromise the security to the Department of Homeland Security.

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

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

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

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

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

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

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

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

_____ _____

DATE NAME *(Last, First, Middle I.)*

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

_____ _____

DATE WITNESSED BY - Department of Homeland Security

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:

$R = P * C$

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 missions areas, affect one or two consequence areas or have a reasonable ability to recover in a timely manner. Marginal criticality targets may not support any mission areas, may have limited to minimal effects of destruction and may have back-up or redundant systems in place that minimize recovery time.

Table 1: Criticality Assessment

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

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

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

STEP 2: THREAT ASSESSMENT AND SCENARIO SELECTION

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

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

Table 2: Notional List of Scenarios

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

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

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

STEP 3: CONDUCTING A CONSEQUENCE AND VULNERABILITY ASSESSMENT

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

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

Table 3: Consequence Categories

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

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

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

Table 4: Consequence Score

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

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

Table 5: Vulnerability Categories

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

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

Table 6 Vulnerability Score

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

STEP 4: CATEGORIZING THE TARGET/SCENARIO COMBINATIONS

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

Table 7. Vulnerability & Consequence Matrix

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

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

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

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

STEP 5: DETERMINING MITIGATION STRATEGIES AND IMPLEMENTATION METHODS

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

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

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

Table 8: General Strategies and Goals for Risk Reduction

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

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

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

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

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

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

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

Table 9: Mitigation Strategy Development Worksheet – EXAMPLE

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

Table 10: Mitigation Strategy Benefit Analysis – EXAMPLE

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

Port Security Assessment

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