U.S. Department of Transportation
United States Coast Guard

Commandant
United States Coast Guard

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

COMDTPUB P16700.4
NVIC 9 02
SEP 30 2002

NAVIGATION AND VESSEL INSPECTION CIRCULAR NO. 9 02

Subj: GUIDELINES FOR PORT SECURITY COMMITTEES, AND PORT SECURITY PLANS REQUIRED FOR U.S. PORTS

Ref: (a) Marine Safety Manual Volume VII, Port Security, COMDTINST M16000.12
(b) Magnuson Act of 1950 and Executive order 10173, as amended
(c) Ports And Waterways Safety Act (PWSA) of 1972
(d) Risk-Based Decision-Making Guidelines, COMDTINST M16010.3
(e) COMDT COGARD Washington DC 172345 DEC 01
(f) PDD-63 Critical Infrastructure Protection
(g) HSPDD – 3 Homeland Security Advisory System
(h) DOT Report to Congress, "An Assessment of the U.S. Marine Transportation System" dated September 1999
(i) Navigation and Vessel Inspection Circular No. 1-00, Guidance for the Establishment and Development of Harbor Safety Committees Under the Marine Transportation System (MTS) Initiative, COMDTPUB P16700.4
(j) Guidance for Coast Guard Coordination of Marine Transportation System (MTS) Improvement Efforts at the Regional and Local Level, COMDTINST M16010.9
(k) Interagency Commission on Crime and Security in U. S. Seaports, August 2000
(l) COMDT COGARD Washington DC R281216Z MAY 02/ALCOAST 258/02, G-CCS
(m) 49 CFR 1520 TSA Regulations: "Protection of Sensitive Security Information"
(n) Contingency Preparedness Planning Manual, COMDTINST M3010.13 (series)

DISTRIBUTION – SDL No. 139

	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
A																										
B		2	10		1			1						132	1			1								30
C												1														
D	1	1		1							1															
E															1											
F																										
G																										
H																										

*NON-STANDARD DISTRIBUTION: B:a Commandant (G-MP/G-MOC/MO-1//MSE/MW/OPD/OPL/OPF-3) (1)

1. PURPOSE. The purpose of this Circular is to provide guidance to field commanders on how to develop Port Security Committees (PSC) and Port Security Plans (PSP). The specific goal of this guidance is the formal creation of Port Security Committees and Port Security Plans for U. S. ports. A secondary purpose of this circular is to provide Commanding Officers of Coast Guard Activities, Marine Safety Offices and Captains of the Port (COTP) with a document that addresses port security issues to be shared with the port and maritime community.

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

3. DIRECTIVES AFFECTED. None.

4. BACKGROUND.

   a. Port Security has long been a responsibility of the U.S. Coast Guard. This responsibility has been addressed in a number of U. S. laws. The Magnuson Act of 1950 amended by Executive Order 10173 clearly established the Coast Guard's role on port security (reference (b)).The Ports and Waterways Safety Act of 1972 reaffirmed the Coast Guard's authority and responsibility (reference (c)). These authorities have become even more important in addressing the nation's security in today's environment. The terrorist attacks of September 11, 2001 have re-awakened the nation to the reality that we are not isolated from world events and that our country is vulnerable to terrorist attacks. Reports and studies including "The Interagency Commission on Crime and Security in U. S. Seaports," have identified our ports, waterways and coastal areas as being particularly vulnerable. This is not a new concept to the U.S. Coast Guard or to the users of the U.S. Marine Transportation System (MTS). The Coast Guard, along with other federal, state and local agencies and environmental groups, emergency response organizations, and port stakeholders have worked together in the past through a variety of official and voluntary partnerships and committees to address issues of safety and security. The terrorist attacks of September 11, 2001 have compelled the Coast Guard to re-evaluate and strengthen our abilities to protect the nation's ports, waterways, and coastal areas from possible attack. Port Security Committees or Security Subcommittees of Harbor Safety Committees will bring together Marine Transportation System representatives in port areas with the specific objective of Maritime Homeland Security (MHLS).

b. In December 2001, the Commandant reaffirmed the Coast Guard's Maritime Homeland Security mission. The mission is to work in coordination with the Department of Defense (DOD), federal, state, and local agencies, owners and operators of vessels and maritime facilities, and others with interests in our nation's MTS to detect, deter, prevent, and respond to attacks against U. S. territory, population, and critical maritime infrastructure by terrorist organizations. The mission has been expanded to include five goals: build Maritime Domain Awareness (MDA); ensure positive/controlled movement of High Interest Vessels; enhance presence and response capabilities; protect critical infrastructure and enhance Coast Guard Force Protection; and increase domestic and international outreach. Coast Guard Headquarters is in the final stages of completing a Maritime Homeland Security strategy, which may modify or replace these current goals. This strategy will be distributed under separate cover when approved. To accomplish this mission and goals, among other actions, he directed that port security committees (PSC) or security subcommittees of existing harbor safety committees be formed in each major port. He further directed that Port Security Plans (PSP) be developed and exercised. This NVIC provides direction to COTPs and identifies some tools to assist in establishing PSCs and developing and exercising PSPs.

c. In January 2002, the Coast Guard held a public meeting in Washington, D.C that included a Port Security Workgroup. Among the attendees were national and international marine industry representatives. They collectively expressed the urgent need for port security planning. Their comments indicated the need for specific threat identification, analysis of port threats, and methods for developing performance standards to plan for response to maritime and port threats. Additionally, the public comments stressed the importance of uniformity in the application and enforcement of requirements and the need to establish threat levels with a means to communicate threats to the maritime industry. The meeting docket can be accessed by searching for docket number 11137 on the Docket Management System (DMS) website (http://dms.dot.gov/search).

d. In February 2002, maritime security initiatives were proposed at the International Maritime Organization's Maritime Safety Committee (MSC) Intersessional Working Group meeting, including the development of a maritime security code, which could be incorporated in the International Convention for the Safety of Life at Sea (SOLAS). Recommendations and proposals from the Intersessional Working Group were considered at the MSC's May 2002 session. The U.S. has provided written proposals to IMO to continue its work toward adoption of uniform security requirements. As stated, key to these proposals is the emphasis on port security. The draft security code and regulations will be presented to the assembly at IMO in December 2002, for formal adoption.

5. DISCUSSION.

a. The COTP is responsible for establishing Port Security Committees (PSC). If practical these should be Security Subcommittees of Harbor Safety Committees. The PSC's activities should be coordinated with any Port Readiness Committees serving the same ports. The PSC under the leadership of the COTP will develop and exercise Port Security Plans (PSP). This circular is designed to provide guidance that will maximize consistency while retaining the COTP's flexibility for implementation.

b. The responsibility for MHLS is added to the existing responsibilities for chairing or participating in many other planning and response committees. Each of these existing committees has its own responsibilities. While some COTPs have separate committees for each mandated or recommended committee structure, others have decided to combine committees to address particular issues or have combined committees to work on many issues focusing instead on regional or local geographic areas. A Port Security Committee can be developed by the COTP as best fits the needs of the port community.

c. The purpose of the PSC is to provide a framework to communicate, identify risks, and coordinate resources to mitigate threats and consequences. The COTP will work with Coast Guard units (including Groups, Stations, and Air Stations), DOD, federal, state and local agencies, and owners and operators of vessels and facilities, and other MTS stakeholders, including port authorities, service providers, labor, and recreational boating communities. It is essential that the port community cooperate to detect, deter, prevent, and respond to attacks against U.S. territory, its population, and MTS components. This group should consider attacks that would cause disruptions affecting political, economic, public safety, environmental or defense operations. The PSC should consider the MTS infrastructure defined in "An Assessment of the U. S. Marine Transportation System" and in Presidential Decision Directive 63 "Critical Infrastructure Protection." For the purpose of this NVIC the COTP and PSC have flexibility in defining the port boundaries. A very broad definition of port as "...a developed area of maritime commerce in the U. S." was given at the January 2002 public workshop. Port Security Committees should coordinate their activities with Port Readiness Committees in ports where both committees have responsibility. Enclosure (1) to this NVIC provides a general description of a PSC. One of the responsibilities of the PSC is to formalize stakeholders' roles and responsibilities under various threat conditions by preparing Port Security Plans.

d. The Port Security Plan fits into a "family of plans" concept that will also include the development of security plans for certain marine facilities and vessels using U.S. ports. Together, the execution of these plans will ensure the security of the nation's MTS. The PSP may be developed by the PSC to complement other security plans. It will provide a means to address issues not covered by other

plans. The PSP or PSPs developed by the COTP and port community must address the entire AOR. Enclosure (2) provides non-binding guidelines in the form of a template for developing PSPs. PSPs will also be used to satisfy the evolving domestic and international port security requirements. The international requirements are anticipated to be finalized in December 2002. Therefore, specific plan content guidance will be updated after the December IMO meeting to meet the July 2004 requirement for port facility plans. The guidance in this document has been closely coordinated with international efforts. The proposed international requirements can be read at http://www.uscg.mil/hq/g-m/nmc/imosec/imosecrep.pdf. In order to meet the anticipated international requirement, Port Security Plans will be submitted to Area Staffs by December 2003, and approved by July 2004.

e. The COTP has discretion on how to document the plan produced through the PSC. The PSP should contain the elements addressed in enclosure (2) to ensure security procedures are understood throughout the AOR. This can be accomplished through one regional port security plan, a PSP with sub-plans, individual local security plans, or it can be incorporated as an annex to an Integrated Contingency Plan such as a "one-plan." The use of the Coast Guard 9700/9800 series Operation Plan (OPLAN) is another option. However, the PSP is a coordination tool for the port community and must be available to all of the appropriate law enforcement and port agencies with port security responsibilities. An annex to the OPLAN may be needed to address Coast Guard responsibilities and resource deployment.

f. The first stage of the PSP process will normally begin with the PSC conducting a security assessment of the port area. Enclosure (3) includes a tool that should be used for this assessment. Further information on risk-based decision-making is available in reference (d). The plan should provide for coordinated scalable actions to detect, deter, prevent and respond to threats at varying threat levels. The Coast Guard has established Maritime Security (MARSEC) levels 1, 2, and 3 to describe increasing threat levels and corresponding activities to meet the threats. MARSEC levels are aligned with the Office of Homeland Security's Advisory System (HSAS). Once the assessment process is complete and highest risk areas or issues are identified, the PSC should concentrate on strategies to lessen the risks. The plans must include strategies for each MARSEC level. Scalable actions may include pre-determined actions to be taken by both Coast Guard and other members of the Port Security Committee. This can include deployment of Boarding Teams to provide a Sea Marshaling function, Maritime Safety and Security Teams, and development of regulated navigation areas, security zones, Naval Vessel Protection Zones, and Army Corps of Engineers (ACOE) restricted areas, which are pre-approved and are triggered by changes in the MARSEC level. Recognizing that no single entity has adequate resources to protect port areas and their associated MTS, it is essential that DOD, other federal agencies, local and state agencies and private industry voluntarily contribute

resources to plan and implement strategies. MHLS is an "all hands evolution." One of the main goals of the PSCs is to coordinate, through the plan, the activities of multiple resource providers.

g. Each COTP has completed a Port Security Risk Assessment Tool (PSRAT) evaluation. This evaluation is an internal assessment based on national security priorities. The assessment completed as part of the PSC is a local assessment based on priorities set by the community. The COTP will have to consider the PSRAT results when developing strategies for deploying resources. Currently, G-MP is developing "Port Security Assessments" and "Port Security Self-Assessment" methodologies, which the COTP can use to augment the security assessment done by the PSC and to refine the PSP. This will allow the COTP to ensure resources are targeted against greatest consequences and vulnerabilities and ensure the necessary risk areas are reduced by the actions documented in the PSP. The PSPs shall be reviewed and updated as necessary from the results of any security assessment, including those designated militarily and economically strategic ports for which a comprehensive port security assessment will be conducted by a contractor with Coast Guard Headquarters' oversight within the next three years.

h. The final stage in the planning cycle is the training, exercising and evaluation phase. In order for a plan to be useful, it must be practical; each entity with responsibility under the plan must understand its role and how to communicate effectively with other members of the team. To accomplish this, individuals identified as having a role under the PSP must be trained and the plan must be exercised. Active evaluation of the plan as written and as executed during exercises or actual incidents is essential to ensuring success. The PSC must coordinate and undertake an evaluation of the plan and its execution. The evaluation and exercise phase is key to an iterative process aimed at continuously improving the PSP.

i. PSCs will discuss sensitive security issues and will document these. Therefore, PSPs will contain sensitive security information (SSI). Reference (l) provides guidance on implementing the Coast Guard's sensitive security program. This program is authorized by Transportation Security Administration (TSA) regulation (reference (m)). The provisions for working with this information closely follow the method in place for safeguarding "For Official Use Only (FOUO)" information.

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

6. IMPLEMENTATION.

a. In a December 17, 2001 message to Coast Guard units, the Commandant of the Coast Guard directed COTPs to "form port security committees or security subcommittees of existing harbor safety committees in each major port." In accordance with the Commandant's order, PSCs should already be in place in major ports. This NVIC expands the Commandant's direction to all COTPs to establish and charter Port Security Committee(s) in all port areas necessary to provide security coverage to the entire AOR.

b. Coast Guard Area and District Commanders shall work with COTPs to establish scalable port security regulations based upon the input received from the PSC(s) and the COTP. These regulations may include Regulated Navigation Areas with a port security component, security zones activated only during heightened threat conditions, or other combinations of field regulations issued under 33 CFR Part 165. Ultimately, these port security regulations will allow for quick implementation of security requirements and procedures to be taken within the port. By publishing these actions ahead of time, the maritime public can incorporate any navigational changes into their business schedule. At no time would these regulations prevent a COTP from taking more extensive measures within their port in times of national emergency or imminent attack, pursuant to existing authority.

c. A template for Port Security Plans is included in enclosure (2). While not mandatory, using the template will help to keep plans uniform and enhance overall efficiency.

d. In accordance with this circular, the COTP working through PSC(s) shall, by February 28, 2003:

1) Conduct a preliminary port level security assessment (enclosure (3));

2) Identify, develop, and "game" scenarios focused on port-specific aspects of the MTS;

3) Develop strategies to increase awareness, decrease vulnerability, increase response readiness, and mitigate consequences in each security level;

4) Identify shore-based and maritime security resources and their functional capability;

5) Begin development of initial port security plan(s) or annexes of existing plans focused on each Maritime Security level, using the port level security assessment developed by the PSC;

6) Identify gaps in Coast Guard resources for each MARSEC level and include them in Regional Strategic Assessments (RSAs).

7) Submit an interim report, via the chain of command, to the Area Commander with a copy to G-MP and G-MOR to be used to analyze resource needs, possible legislation change proposal requirements, and allow for reprogramming of funds or supplemental funding. The interim report shall include:

- Relationship of PSC, if any, to other committees, including, but not limited to, Harbor Safety Committee(s), Port Readiness Committee(s), and Area Committees;
- Description of how plan addresses entire AOR.
- PSC membership, by agency;
- Legal or regulatory challenges encountered and needing national review;
- Success stories/best practices that may be beneficial to other PSCs;
- Any significant lessons learned;
- Resource and capability shortfalls and measures to address gaps.

c. Each COTP shall use the enclosed guidelines to develop a port security plan or plans. These plans may be part of another plan as long as the entire COTP zone is considered and requirements for port level assessment, description of security procedures for each MARSEC level, and other elements of the template in enclosure (3) are met.

f. Finally, I anticipate that PSCs will need to access or produce information that is security sensitive. The ultimate goal is to have the majority of the plan unclassified. However, there may be classified annexes, and the entire plan will likely be considered security sensitive. Therefore, the COTP shall ensure classified material is not inadvertently disclosed and proper procedures for handling security sensitive information are explained and followed. G-MP will be preparing a classification guide for PSPs to assist the COTPs in determining which parts of the Plan should be Sensitive Security Information, or Classified, and specific classifying authority requirements for this material.

PAUL J. PLUTA
Assistant Commandant for Marine Safety, Security and Environmental Protection

DAVID S. BELZ
Assistant Commandant for Operations

Encl: (1) Guidance for Development and Management of Port Security Committees (PSC)
(2) Port Security Plan Development Guidance
(3) Port Level Assessments

Subject: GUIDANCE FOR DEVELOPMENT AND MANAGEMENT OF PORT SECURITY COMMITTEES (PSCs)

Ref: (a) COMDT COGARD Washington DC 172345Z Dec 01
(b) An Assessment of the U. S. Marine Transportation System – A Report to Congress, September 1999
(c) Report of the Interagency Commission on Crime and Security in U. S. Seaports, August 2000
(d) National Oil and Hazardous Substances Pollution Contingency Plan, 40 CFR 300
(e) CG – FBI MOU Concerning A Policy of Mutual Assistance in Support of CG/FBI Operations to Counteract Terrorist Activities in a Maritime Environment
(f) Navigation and Vessel Inspection Circular 1-00, Guidance for the Establishment and Development of Harbor Safety Committees Under the Marine Transportation System (MTS) Initiative, COMDTPUB P16700.4
(g) Guidance for Coast Guard Coordination of Marine Transportation System (MTS) Improvement Efforts at the Regional and Local Level, COMDTINST 16010.9
(h) COMDT COGARD Washington DC 281216Z MAY 02/ALCOAST 258/02, G-CFI

BACKGROUND.

The concept of local area coordination for awareness, planning, prevention and response (e.g. Area Committees and Harbor Safety Committees) has been practiced with great success by Coast Guard Captains of the Port (COTP). The formation of Port Security Committees (PSCs) expands on this proven concept to cover the national security issues brought to the fore by the attacks against the United States on September 11, 2001. The Commandant required the establishment of Port Security Committees in reference (a). The requirement is extended by this NVIC to include PSCs for all port areas as deemed necessary by the local COTP.

The Report of the Interagency Commission on Crime and Security in U. S. Seaports published in August 2000, reference (c), recommended that the Coast Guard act as the lead agency in "strengthening interagency, intergovernmental, and public/private sector efforts to address the threats of seaport crime (including terrorism)..." The Commandant accepted this role when he testified before the U. S. Senate's Committee on Commerce, Science and Transportation in October 2000. The Department of Transportation's Report to Congress, reference (b), also addresses the threats of seaport crime including terrorism. Both reports lay excellent groundwork in discussing the threats to national security and crime existing in the Marine Transportation System (MTS) in general and in port areas in particular. The September 11 attacks have highlighted the need to focus the nation's attention on terrorism.

DISCUSSION.

The Coast Guard's Maritime Homeland Security (MHLS) mission to deter, detect, prevent and respond to attacks against U. S. territory, population, and critical maritime infrastructure by terrorist organizations can best be accomplished through interagency, intergovernmental and public/private sector cooperative efforts. The Coast Guard as lead agency will accomplish its mission in part through Port Security Committees (PSCs). PSCs will be established and led by COTPs. They will provide a framework to communicate threats, identify risks, and coordinate resources to mitigate threats and vulnerabilities.

The most urgent actions to be taken by the PSC are the development (including port risk assessments), review, and update of a Port Security Plan. The Port Security Plan is a living document that should be updated as necessary to reflect the changing security posture of the port community. It should be noted that the PSC is responsible for planning and coordination for security procedures and is not to be considered a response entity for the purposes of consequence management. However, the links between the PSC and Area Contingency Committees are crucial to improving overall preparedness.

The PSCs are comprised of federal, state, and local agencies, law enforcement and security agencies, and port industry stakeholders. The PSCs provide a regular and active forum for the enhancement of security and the prevention of criminal activity (including terrorism) within ports, waterways and coastal areas.

When developing the local membership and organization of the PSC, COTPs should take into account all of the aspects of the MTS as applicable for each port area and its adjacent waterways and coastal areas. As defined in reference (b), the MTS consists of:

- waterways, including associated infrastructure (e.g. locks and dams, bridges, aids to navigation);
- ports (e.g. marine transportation facilities where vessels transfer cargo and people, and recreational waterfront facilities and shipyards);
- intermodal connections (e.g. pipelines, road and rail access routes);
- vessels and vehicles;
- MTS users (e.g. commercial, recreational and defense related);
- MTS support systems
    - information systems (e.g. Intelligent Transportation Systems, communication systems and marine information systems); and
    - port management systems (e.g. Vessel Traffic and Monitoring Systems, and Cargo manifest systems); and
- power and water distribution systems.

Representatives for each aspect of MTS and those who are charged with the regulation or enforcement of these should be encouraged to participate.

For example PSC membership could include (but not be limited by):

- Federal Government representatives
  - US Coast Guard (COTPs (chair)), Groups, Air Stations and Small Boat Stations, VTS, MSSTs)
  - Federal Bureau of Investigation (FBI) (Lead Federal Agency (LFA) for federal response to terrorist incidents – crisis management)
  - Federal Emergency Management Agency (FEMA) (Lead Federal Agency – consequence management)
  - US Customs Service
  - Immigration and Naturalization Service (INS)
  - Transportation Security Administration (TSA)
  - Department of Defense (DOD)
    - US Transportation Command (TRANSCOM), Military Sealift Command (MSC), Military Traffic Management Command (MTMC)
  - Environmental Protection Agency (EPA)
  - US Department of Agriculture (USDA)
  - Animal and Plant Health Inspection Service (APHIS)
  - Occupational Safety and Health Agency (OSHA)
  - Maritime Administration (MARAD)
  - Research and Special Programs Administration (RSPA)
  - Federal Railway Administration (FRA)/Federal Highway Administration (FHWA)/ Federal Transit Administration (FTA)
  - Army Corps of Engineers (ACOE)
  - Other government representatives, where appropriate
- Emergency Management and Law Enforcement Agencies
  - Local, county and state police and government officials
  - National Guard
  - Port Authority police and/or security forces
  - Terminal/facility security force
  - Marine Police
  - Fish and Wildlife marine units
  - Fire Departments
- Other State, Local and City Government representatives
  - State Department of Natural or Environmental Resources marine units
  - Other Environmental Agencies
  - City government officials
  - Health Agencies
  - Occupational Safety Agencies
  - Transportation Agencies
  - Regional Development Agencies/Metropolitan Planning Organizations
- Port Authorities
- Civil Defense

- Vessel owners/operator security representatives
- Facility Owner/Operators
- Terminal Owner/Operators
- Trade organizations
- Recreational Boating organizations (Yacht Clubs, rowing clubs)
- Pilot Associations
- Railroad Companies
- Trucking Companies
- Shipyards
- Tow Boat operators
- Marine Exchanges
- Industry Organizations
- Organized Labor
- Commercial Fishing Industry
- Other Facilities within the port having waterside access (e.g. refineries, chemical plants, power plants)

Other existing port planning and response committees have their own strategic goals and focus. PSCs are established to address issues directly involving Maritime Homeland Security (MHLS). Just as jurisdictions in the ports are overlapping, some committee responsibilities may overlap. For example, MHLS encompasses national security objectives pertaining to the MTS, including the need to support military operations conducted through the ports by Department of Defense. These issues have been directly addressed by the Port Readiness Committees (PRCs) and the National Port Readiness Network (NPRN). Coordination will need to exist between the PSCs and PRCs. Some committees such as the Harbor Safety Committees (HSC) have sub-committees or ad hoc committees in place already working on port security issues. COTPs may decide to expand HSCs to form Port Security sub-committees, establish the PSC as a subcommittee of another existing committee or establish existing PRCs under new PSCs. PSCs shall be led by COTPs. Regardless of the organization, the COTP is responsible for coordinating the MHLS activities of their appropriate committee or subcommittee.

The structure of the PSC is not mandated, however, from experience the organization of Area Committees under the National Contingency Plan (reference (d)) offers a successful example. This structure was closely followed by Harbor Safety Committees and is detailed in reference (f).

A recommended general organizational structure may be applied to most PSCs. While particular elements of PSC structures may differ from port to port, PSCs may be organized into a tiered organization consisting of a managing board or steering committee, general committee and ad hoc or standing committees. A general committee of the PSC should be open to participation by all interested port stakeholders. A managing board should be made up of representatives of agencies that the COTP determines have the authority necessary to enact or enforce the scalable activities and procedures decided to be appropriate at each MARSEC level. Managing board members could also include representatives of agencies that have resources that could be utilized in port security related function or mission. Ad hoc or standing committees may be made up of people from the general committee. They can work on issues raised by the general committee or by the managing board. The managing board oversees the day-to-day scheduling and operations of the PSC, and coordinates the agenda.

Much of the work that the PSC will undertake will involve sensitive security information. The Department of Transportation has established a new category of information entitled Sensitive Security Information (SSI). It is not classified material but it will have some restrictions on its handling and distribution. The Coast Guard's initial procedures for SSI are published in reference (h). The COTP is responsible for developing procedures to protect both SSI and classified information that is developed and used by the PSC. The managing board may consider and evaluate SSI and classified information on behalf of the general committee. When possible, managing board members should be persons with valid security clearances. Only individuals with appropriate security clearances may have access to classified information.

Initially the full committee (managing board, general and sub committees) may meet on a quarterly basis. As chair, the COTP is responsible for notifying all members of meeting logistics. More frequent meetings of the managing board and sub-committees may be held during initial plan development or to respond to special circumstances, significant changes in port operations such as a new dangerous cargo or to changes in threat levels.

The managing board or steering committee may meet quarterly in conjunction with the full committee or at other times as needed.

(SAMPLE Port Security Plan)

Subject: PORT SECURITY PLAN DEVELOPMENT GUIDANCE

BACKGROUND.

The Coast Guard is employing a "family of plans" concept to ensure security in our nation's port, waterways and coastal areas. This enclosure addresses the Port Security Plan (PSP).

The Coast Guard's "family of plans" regarding security includes the PSP, commercial Vessel Security Plan and commercial Facility Security Plans. The PSP should cover port areas and adjacent waterways, coastal areas and Marine Transportation System (MTS) infrastructure.

The Port Security Committee (PSC) should develop the PSP.

DISCUSSION.

The PSP is primarily a communication and coordination document. It will be developed from port security assessments, and will describe the risk and vulnerability reduction security procedures to be implemented at each Maritime Security (MARSEC) level.

How to Use the PSP Template:

This template is designed to be adapted and used by PSCs in preparing Port Security Plans. It should be able to provide enough information for the port community to understand and implement the pre-determined security procedures for each MARSEC level.

The template has placeholders for local names or identifiers. They appear [*italicized in brackets.]*

It also has explanatory language that may be helpful in understanding the contents of a particular section. They may be omitted in the final plan. These appear (*italicized in parentheses).*

(SAMPLE Port Security Plan)

(This example plan is provided to facilitate plan development at the port level. Use of this format is not mandated, but is encouraged to ensure plan similarity between port areas.)

(Color of cover should correspond to guidance in COMDTINST M3010.11B. i.e. Blue unclassified; Yellow confidential; Red Secret)

PORT SECURITY PLAN
for
[*insert name of port area covered*]

[*If sub-plan, then state plan affiliation.]*

developed by
[*insert name of Port Security Committee or Security Subcommittee of Harbor Safety Committee or Port Readiness Committee]*

Promulgated on
[*insert date approved*]

(SAMPLE Port Security Plan)

Record of Distribution

Agency	Date

(SAMPLE Port Security Plan)

Record of Changes

Change	Section	Initials Date

(SAMPLE Port Security Plan)

Table of Contents

Record of Distribution
Record of Changes
Table of Contents

1000. Introduction
- 1010. COTP Letter of Promulgation (*may include a signature page)*
- 1020. Purpose
- 1030. Assumptions
- 1040. Situation

1100. Port Security Committee
- 1110. Charter
- 1120. Organization & Membership
- 1130. Relationship to Other Planning and Response Committees

1200. Port
- 1210. Port Physical Characteristics
- 1220. Port Economic Characteristics
- 1230. Reference Charts or Maps *(may be appendices)*

2000. Security Operations
- 2100. Awareness (Detect)
  - 2110. Port Security Assessment *(enclosure 3)*
    - 2111. Identify activities and critical operations
    - 2112. Define Scenarios
    - 2113. Conduct Consequence and Vulnerability Assessment
    - 2114. Prioritize Scenarios
- 2200. Prevention (Deter) & Mitigation
  - 2210. Maritime Security (MARSEC) Levels
    - 2211. Communicating MARSEC Levels
    - 2212. Coordinating MARSEC Levels
  - 2220. MARSEC Level 1
    - 2221. Security Procedures
    - 2222. Roles, Resources, Authorities and Responsibilities
    - 2223. Gaps & Actions to Mitigate
  - 2230. MARSEC Level 2
    - 2231. Security Procedures
    - 2232. Roles, Resources, Authorities and Responsibilities
    - 2233. Gaps & Actions to Mitigate
  - 2240. MARSEC Level 3
    - 2241. Security Procedures
    - 2242. Roles, Resources, Authorities and Responsibilities
    - 2243. Gaps & Actions to Mitigate

2300. Relationship of Port Security Plan to Other Security Plans
- 2310. Facility Security Plan
- 2320. Vessel Security Plans
- 2330. Passenger Vessel Terminal Security Plans
- 2340. Passenger Vessel Security Plans
- 2350. Adjoining Port Security Plans
- 2360. *(other security plans)*

2400. Response & Crisis Management
- 2410. Relationship of Port Security Plan to Response Plans
  - 2411. National Oil and Hazardous Material Spill Response Plan
  - 2412. Area Contingency Plan
  - 2413. Maritime Counterterrorism Contingency Plan
  - 2414. United States Government Interagency Domestic Terrorism Concept of Operations Plan (CONOP)
  - 241X. *(other response plans)*

2500. Consequence Management
- 2510. Relationship of Port Security Plan to Consequence Management Plans
  - 2511. Federal Response Plan
  - 2512. Natural Disaster Plans
  - 251X. *(other consequence management plans)*

3000. Plan Documentation
- 3100. Plan Review & Comment
- 3200. Plan Security and Control

4000. Port Security Training

5000. Port Security Exercise Program

6000. Appendices *(Appendices may be used to segregate classified information. They may also be used to document specific geographic, infrastructure (physical or cyber), port or vessel services, or industry security procedures. Information in this section may be incorporated or referenced as a separate document as appropriate).*

(Examples of appendices:)

6100. (Unclas) Port Security Committee Member Entities, Representatives & Contact Info
6200. (Classified or SSI) Charts and Maps With ID of Port Tenants & Infrastructure
6300. (Classified or SSI) Port Operations and Infrastructure
6400. (Classified or SSI) Risk Based Scenarios
6500. (Classified or SSI) Security Procedures
    6510. Risk ranked infrastructure for consequence categories
    6520. Setting MARSEC conditions
    6530. Actions for MARSEC conditions
    6540. Utilization of security resources
    6550. Communications Plan
    6560. Procedures for Breach of Security
    6570. Types of Existing Valid Identification
6600. (Classified or SSI) Dangerous Cargoes for Security Planning.
6700. Quick Response Cards For High Risk Scenarios
6800. Agency/Organizational Questionnaire. *(This optional form may be used in the PSC development process. This information can be incorporated into the plan.)*

Glossary/Definitions
Index

(SAMPLE Port Security Plan)

1000. Introduction

The Port Security Committee for the Port of *[insert location]* has created this Port Security Plan. The stated purpose of the Port Security Committee and the Port Security Plan is to provide a framework for communication and coordination to identify threats and reduce vulnerabilities to terrorist actions in and near the Marine Transportation System.

1010. COTP Letter of Promulgation *(may include a signature page)*

1020. Purpose

The U.S. Coast Guard is the lead federal agency for the Maritime Homeland Security mission. In this capacity, the Captain of the Port (COTP), as the Coast Guard's lead entity in the port is responsible, through the Port Security Committee (PSC), for developing a Port Security Plan (PSP). The PSP defines the government's (local, state and federal) obligation and the other port stakeholders contributions to the Maritime Homeland Security mission. The PSP is designed to capture the information necessary to coordinate and communicate security procedures at each Maritime Security (MARSEC) level. The plan's goal is to enhance awareness for the detection of terrorist threats, to deter attacks, and reduce vulnerabilities through coordinated security procedures and communication. The PSP will complement facility and vessel security plans. Because the PSP's purpose is prevention, it must also integrate with (and may cause revisions to) existing plans for response (e.g. Area Contingency Plans (ACP), 9700/9800 series Operational Plans (OPLANs)) and consequence management (e.g. Federal Response Plan (FRP)) when incident response and consequence management are necessary.

1030. Assumptions

1. No single private or government entity at the local, State or Federal level possesses the authority, the resources and the expertise to act unilaterally on the difficult issues that may arise in response to threats or acts of terrorism.
2. A terrorist incident may occur at any time of day or night with little or no warning.
3. Each entity directly or indirectly involved with the Marine Transportation System (MTS) will voluntarily participate with the Port Security Committee to increase awareness and enhance prevention of terrorist acts.
4. The National Oil and Hazardous Material Contingency Plan, Federal Response Plan, and other response plans will be activated for the purpose of response and consequence management due to a terrorist incident.
5. Protection of human life, health, and security is the most important consideration in plan development and execution.
6. Maintaining commerce in the port area is a critical consideration.

7. *(List other assumptions, if any)*

1040. Situation

The complexity, scope and potential consequences of a terrorist threat or incident occurring in or near our Marine Transportation System (MTS) require that there be a coordinated effort between all port users and law enforcement agencies. This effort will require open communication and enhanced awareness of potential threats. It will also require all those involved to fully understand their roles in enhancing security. The Coast Guard and international maritime community have developed a tiered maritime security system (MARSEC) consistent with the Office of Homeland Security's Homeland Security Advisory System (HSAS).MARSEC is specifically designed to alert users of the MTS. Through this plan the stakeholders of the MTS (described in subsequent paragraphs) agree to take certain actions contingent upon the Coast Guard's activation of MARSEC levels.

1100. Port Security Committee

1110. Charter

The Port Security Committee for the Port of *[insert port area name]* is hereby chartered effective *[insert date]*.

The Committee is composed of government agencies, commercial entities and other groups or individuals interested in preserving and improving the security of our shared waterfront areas and Marine Transportation System (MTS). Committee membership and participation will be at the discretion of the COTP.

The Committee has been created to build awareness of potential threats to port areas, and identify those threats; to protect the port through improved security procedures and communication, and to coordinate security procedures to decrease port vulnerabilities.

The objectives of the committee include:

1. Develop a Port Security Plan (PSP) aimed at maintaining acceptable risk levels during normal operations and during times of heightened threats. This plan will outline scalable security procedures to be taken by MTS stakeholders to ensure the continued safety and security of our nation's port areas and MTS.
2. Integrate, and/or amend, existing security assessments of maritime facilities using agreed criteria. Assessments to be used to determine appropriate facility security measures.
3. Develop and adopt preventative security measures for appropriate Maritime Security Level 1 (sustainable baseline) and Levels 2 and 3 to address increased threat conditions (both general and specific). The measures will meet consolidated requirements of all agencies having jurisdiction. The measures will be used to influence interim and future regulations.

4. Develop procedures for information sharing for threat warnings, response, intelligence-gathering and threat assessment among public and private entities
5. Produce stakeholder recommendations for continuing improvements for port security measures.
6. To the extent possible, promote effective security measures that maintain or enhance operational efficiencies and minimize impact to trade.

1120. Organization & Membership

The Port Security Committee (PSC) for *[insert port area name]* is chaired by the U. S. Coast Guard Captain of the Port, *[insert Rank, Name, contact info]*, who is also designated as the Port Facility Security Officer (PFSO).

(The COTP will serve in the function of PFSO to satisfy the developing international requirements.)

[Insert Port Security Committee organization (steering committee; general committee, standing & ad hoc committees.]

[Insert committee membership for this port area; processes for reviewing committee organization or other by-laws may be included here or as appendices.]

[Insert frequency of PSC meetings (at least 4 times each year)]

1130. Relationship To Other Planning Committees

Other planning committees exist at the port level. The PSC is related to other committees in the port level including: *(if applicable)*

The Port Readiness Committee. (*Include brief description of PRC activities/charter and relationship to PSC).*

The Area Committee for *[Insert name of AC]. (Include a brief description of AC activities/charter and relationship to PSC).*

Harbor Safety Committee *[Insert name of HSC]. (Include brief description of HSC activities/charter and relationship to PSC.)*

(Other committees as appropriate.)

1200. Port

For the purposes of this plan the term "port" means the port area and its adjacent waterways, including Marine Transportation System (MTS) infrastructure, especially the ship/port interface in each Captain of the Port Zone.

1210. Port Physical Characteristics

[Insert a description of the boundaries of the port as defined for the purpose of this plan by the PSC. This should be an identifiable body of water and surrounding waterfront area including MTS infrastructure (both physical and information systems). Ports should be readily identified areas that have a vessel/facility interface and associated waterfront areas.]

(Port Physical Characteristics- Examples:

The Port of Cleveland, Ohio is located on the Southern shore of Lake Erie in the City of Cleveland, Ohio. The "Port" includes all waters internal to the federal break wall and the Cuyahoga River to the head of navigation at mile marker 5.2. This includes all marinas, and waterfront facilities.

The Port of San Francisco Bay is located on the Northern California Coast. The Port includes all tidally influenced waters within the greater San Francisco Bay Area and the offshore areas contained. This includes the waters of San Francisco Bay and the Sacramento/Stockton river delta area and their tributaries. This includes the ports of San Francisco, Oakland, Richmond, Redwood City, Benicia, Stockton and Sacramento and the offshore traffic separation area found in 33 CFR Part...

The Port of (river port) includes all waters and adjacent waterfront from mile marker XX to mile marker XX of the Missouri River, and all waters 1 mile upstream and downstream from the following structures (Bridges, locks, etc.).

Sub-port areas.

Secondary ports within the COTP zone may be a subpart of a larger committee and plan or may be entirely separate.

Example of a sub port: The Port of Ashtabula, Ohio is on the Southern Shore of Lake Erie in the town of Ashtabula, Ohio. This port is considered a sub port of the Cleveland Port Security Committee and Cleveland Port Security Plan.

The following agencies are members of the Cleveland Port Security Committee for Ashtabula matters only:
Ashtabula City Police
Ashtabula Port Authority
Ashtabula County Sheriff
Etc.)

1220 Port Economic Characteristics.

(Briefly describe major port activities, industries and products for the port and all sub ports. The purpose of this section is to educate committee members on major port activities. Some participants may not be aware of maritime operations, navigation areas, major cargoes or MTS infrastructure concerns.)

1230. Reference Charts or Maps

(may be appendices)

2000. Security Operations

The PSP establishes a range of Maritime Security Levels or MARSEC levels determined by the U. S. Coast Guard that serve to frame the nature and scope of security procedures to be followed in response to a recognized threat. Each MARSEC level provides for an escalating range of actions that may be implemented to reduce the risk or vulnerability to a terrorist incident. The COTP will announce changes to the MARSEC level by the means defined in this plan to other port stakeholders. The U. S. Coast Guard and other port stakeholders may then implement the predetermined security procedures defined in this plan and through future regulation.

The three level MARSEC system is tied to the Office of Homeland Security's HSAS warning system. MARSEC Level 1 corresponds to the lowest three levels of the HSAS. These are HSAS Low: Green, HSAS Guarded: Blue and HSAS Elevated: Yellow. MARSEC Level 2 corresponds to HSAS High: Orange. MARSEC Level 3 corresponds to HSAS Severe: Red.

2100. Awareness (Detect)
(The PSP should contain the scenarios evaluated, the results of the evaluation and mitigation measures. Section 2100 documents Steps 1-4 and Section 2200 documents Step 5.)

(The PSP should also identify how the PSC is obtaining maritime domain awareness (MDA) of the people, cargo and vessels with their current capabilities. Note: Coast Guard headquarters is developing the MDA initiative and will be providing further capability in the future.)

2110. Port Security Assessment

The Port Security Committee should conduct a risk-based analysis of their port. The process, as adopted by the U. S. Coast Guard consists of five steps which are explained in enclosure (3) to the "Guidelines for Port Security Committees, and Port Security Plans Required For U. S. Ports" NVIC. The steps are: (1) Identify critical operations and infrastructure; (2) Develop attack scenarios; (3) Conduct consequence and vulnerability assessment for each scenario; (4) Categorize and prioritize; (5) Develop mitigation strategies.

(NOTE: The following sections may contain Classified and Sensitive Security Information (SSI). Note: Coast Guard headquarters is developing SSI and Classification guidance which will be provided under separate cover.)

(Documentation of the Security Assessment may be made in separate appendices.)

2111. Identify Activities and Critical Operations

(Document Targets. Identify those specific infrastructure (physical and cyber) that support critical operations of the port. All identified should be included. Those considered but dismissed for evaluation should be documented for future reference.)

2112. Define Scenarios

(Document Scenarios. 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.)

2113. Conduct Consequence and Vulnerability Assessments

(Document Assessments. Evaluate each target/attack scenario combination in terms of the potential consequences of the attack and the vulnerability of the target to the attack.)

2114. Categorize and Prioritize Scenarios

(Document Prioritization. Determine which scenarios should have mitigation strategies, and also document why other scenarios did not need mitigation strategies, based on the consequence and vulnerability assessment.)

2200. Prevention (Deter) & Mitigation

(Completing the PSP is an important first step to prevention and mitigation. But, it will only be the beginning of the process of upgrading port security. The tiered and scalable security procedures developed by the PSC will likely be a combination of voluntary and mandatory procedures that will be the shared responsibility of the Coast Guard, State and municipal entities and vessels and facilities operating in the port, adjacent waterways or MTS infrastructure.

After the PSP has been completed and approved, the next step, if appropriate, will be to develop a comprehensive set of local and national regulations (and perhaps, other agreements like MOAs with the state) to implement the security procedures set out in the PSP.

To be legally required and enforceable through civil or criminal penalties, those security procedures must be promulgated either in the Code of Federal Regulations (CFR), or Federal Register after appropriate notice and comment procedures.)

2210. Maritime Security (MARSEC) Levels

Maritime Security (MARSEC) levels were established to allow the Coast Guard to easily and clearly communicate the security measures to be taken in response to a HSAS threat. MARSEC levels also permit the COTP and the port community to plan and pre-designate appropriate postures for each level of threat.

2211. Communicating MARSEC Levels

The Coast Guard is responsible for communicating MARSEC levels to the affected port stakeholders. The responsibility for letting the affected port users and law enforcement community members know that there has been a change in MARSEC level (or particular procedures) resides with the COTP. Any change shall be broadcast as described in the PSP.

(Describe the process for broadcasting changes to MARSEC levels. The plan should consider the best distribution system to reach as many people as possible by the most rapid means available.)

(Describe the notification process that MARSEC Level has been set.)

2212. Coordinating MARSEC Levels

The COTP will maintain flexibility in applying security procedures through the process described in the PSP. The COTP shall consider variances from or operational equivalences for security procedures in the PSP.

(Describe procedure for requesting/approving variances from, or operational equivalencies for, the security procedures listed in the plan.)

(Describe procedures for vessels entering port at different security level. i.e. Ship is operating at MARSEC level 1 and port is operating at MARSEC level 2.)

2220. MARSEC Level 1

MARSEC Level 1 (Baseline level of effort, "new normalcy"). Corresponds to Homeland Security Advisory System (HSAS) Low: Green, Guarded: Blue, Elevated: Yellow. This level is the new maritime security normalcy. It is the operational frame of reference that defines the security level required to address the increased general threat level in our ports, harbor approaches, and waterways. This is the risk level for which protective measures must be maintained for an indefinite period of time; in other words, these are the normal, every day security measures.

2221. Security Procedures

(Security procedures developed in the Security Assessment can be discussed here or in appendices.)

1. Establish procedures to share information to allow for more complete knowledge of cargo, people and vessels using port.
2. Plan for/Establish Security Zones and Restricted Zones and Regulated Navigation Areas and who is going to enforce them.
3. Incorporate security elements into duties and responsibilities of all port personnel.
    a. *(Define security elements. Can include routine duties, such as observing and reporting malfunctioning security equipment and suspicious persons, objects.)*
4. Establish restricted areas to control access.
    a. *(Define restricted areas. Can include cargo and ship stores transfer area; passenger and crew embarkation area; locations where ships receive port services.)*
5. Mark restricted areas.
6. Develop restricted area access control policy. (Consider physical means such as barriers and fences.)
7. Monitor restricted areas.
    a. *(Can include locking or securing access points; using surveillance equipment or personnel; automatic intrusion detection devices and by issuing identification passes.*

8. Identify access points to port
    a. *(Can include waterways; rail lines; roadways; walkways; electronic information systems; and adjacent structures)*
9. Develop control measures for access points, (including identification verification, and frequency of application)

(The CG has recently published guidelines in the Federal Register (vol. 67, no.152, pgs. 51082-51083) which describe the requirements for maritime identification credentials. Every person (including foreign seafarers) entering a US port facility, or embarking on or disembarking from a vessel will be required to carry, at a minimum, a laminated (or otherwise secured from tampering)identification card that displays the holder's full name and current photograph and the name of issuing authority or company.)

10. Designate areas to perform control measures
11. Deny access to anyone refusing to submit to security verification
12. Monitor port, including at night and in times of poor visibility
13. Establish procedures and means of communicating any threatening acts
14. Supervise handling of cargo and ship's stores
    a. *(Can include cargo security procedures to prevent tampering; or inventory control procedures at access points.)*

2222. Roles, Resources, Authorities and Responsibilities

(Describe how, and by whom, security procedures will be implemented.)

2223. Gaps & Actions to Mitigate

(Describe any gaps in attaining MARSEC level 1, and the steps being taken to mitigate them, which may include application for grants.)

2230. MARSEC Level 2

MARSEC Level 2 ("heightened risk") Corresponds to HSAS High: Orange. There is a heightened threat of an unlawful act against a port, or vessel and intelligence indicates that terrorists are likely to be active within a specific area or against a specific class of target. The risk level indicates that a particular segment of the industry may be in jeopardy but that no specific target has been identified. Additional protective measures may be expected to be sustained for substantial periods of time.

2231. Security Procedures

(Security procedures developed in the Security Assessment can be discussed here or in appendices.)

1. Continue and enhance security procedures identified for MARSEC Level 1.
2. Review security roles and responsibilities.
3. Control access to restricted areas to allow only authorized personnel.
4. Increase frequency and detail of monitoring restricted areas.
5. Limit the number of access points to port. *(Consider physical means such as barriers and fencing and personnel.)*
6. Increase control of access points to port or other identified areas. *(Consider assigning additional personnel.)*
7. Increase detail and frequency of monitoring of port or other identified areas, including inspection of people, personal effects and vehicles.
8. Increase frequency and detail of supervising handling of cargo and ship's stores.
9. Enhance means of communication to ensure immediate availability.

2232. Roles, Resources, Authorities and Responsibilities

(Describe how, and by whom, security procedures will be implemented.)

2233. Gaps & Actions to Mitigate

(Describe any gaps in attaining MARSEC Level 2, and the steps being taken to mitigate, which may include application for grants.)

2240. MARSEC Level 3

MARSEC Level 3 ("incident imminent") Corresponds to HSAS Severe: Red. The threat of an unlawful act against a port, facility or terminal is probable or imminent. Intelligence may indicate that terrorists have chosen specific targets, though it may not be possible to identify such targets. Additional protective measures are not intended to be sustained for substantial periods of time.

2241. Security Procedures

(Security procedures developed in the Security Assessment can be discussed here or in appendices.)

1. Continue and enhance security procedures identified for MARSEC Levels 1 and 2.
2. Provide security information to all personnel entering port.
3. Communicate with ships and coordinate additional security measures.
4. Monitor restricted areas to protect against an imminent security incident.
    a. *(Can include securing all access points, prohibiting storage of vehicles, cargo and ship's stores, continuous patrols.)*
5. Control access to port. *(Consider enhancing security presence at closed access points, providing escorts, and taking measures to secure locations that overlook port.)*
6. Monitor port to protect against an imminent security incident. *(Consider inspecting all people, personal effects and vehicles).*
7. *Protect electronic information systems.*

2242. Roles, Resources, Authorities and Responsibilities

(Describe how, and by whom, security procedures will be implemented.)

2243. Gaps & Actions to Mitigate

(Describe any gaps in attaining MARSEC Level 3, and the steps being taken to mitigate, which may include application for grants.)

2300. Relationship of Port Security Plan to Other Security Plans

The Port Security Plan is part of a "family of plans." There are other security plans that are specific to facilities and vessels. The "family of plans" concept requires that all security plans be considered in developing the over all security posture for the port.

(If applicable: Include a brief description of plans and relationship to PSP.)

2310. Facility Security Plans *
2320. Vessel Security Plans *
2330. Passenger Vessel Terminal Security Plans
2340. Passenger Vessel Security Plans
2350. Large Passenger Ferry Security Plans
2360. Adjoining Port Security Plans
23X0. *(Add security plans as appropriate. This list does not include all security plans.)*

**(Although individual plans may not be available to the COTP or PSC, general plan requirements will be available in USCG NVICs.)*

2400. Response & Crisis Management

PDD 39 divides the federal response to terrorism into two categories—crisis management and consequence management. Crisis management involves the causes of a terrorist attack; consequence management deals with the aftermath of an attack.

(PDD 39 designates the Department of Justice (acting through the FBI) as lead agency in responding (crisis management) to terrorism in the U.S. An interagency agreement and Memorandum of Understanding were signed by the Coast Guard Commandant and Director of the FBI which describes a mutual support arrangement between the entities for maritime law enforcement activities to counteract terrorist activities. PPD 39 further designates FEMA as lead federal agency in the consequence management phase. The Federal Response Plan addresses further delegation of responsibility for specific types of incident.)

2410. Relationship of Port Security Plan to Response Plans

The Port Security Plan contains information that pertains to prevention of security incidents, such as procedures for communication and coordination to reduce the risk of, or vulnerability to terrorist acts. To be effective when terrorist acts result in security incidents, the procedures detailed in the PSP must be coordinated with incident response plans. Therefore, PSP developers should be mindful of the need to ensure relevant crisis management plans exist for contemplated security incidents, and such plans are referenced in the PSP.

(If applicable: Include a brief description of plans and relationship to PSP).

(PSP developers should consider updating response plans to account for responses under heightened security levels and for resource trade-offs between security and response.)

2411. National Oil and Hazardous Material Spill Response Plan
2412. Area Contingency Plan
2413. Maritime Counter Terrorism Contingency Plan
2414. United States Government Interagency Domestic Terrorism Concept of Operations Plan (CONOP)
2415. 9700/9800 series Plans and Appendices
241X. *(Add response plans as appropriate. This list does not include all response plans.)*

2500. Consequence Management

2510. Relationship of Port Security Plan to Consequence Management Plans

The Port Security Plan contains information that pertains to prevention of security incidents, such as procedures for communication and coordination to reduce the risk of, or vulnerability to terrorist acts. When terrorist acts result in security incidents the procedures detailed in the PSP must be coordinated with consequence management plans.

(If applicable: Include a brief description of plans and relationship to PSP).

2511. Federal Response Plan
2512. Natural Disaster Plans
251X. *(Add consequence management plans as appropriate. This list does not include all Consequence management plans.)*

3000. Plan Documentation

Coast Guard approval of the Port Security Plan is at the Area level. The COTP will review the plan at the port level. After review by the COTP, the plan will be forwarded to Coast Guard Area Marine Safety divisions via the District Marine Safety Officer for further review and approval. Completed plans will be maintained by the COTP.

3100. Plan Review and Maintenance

Plan review is a continuous process. The plan should be reviewed by the PSC on a regular basis (at least annually) for adequacy, feasibility, consistency and completeness. The plan should be reviewed after each activation, exercise and drill. It should be reviewed as port conditions change. After each review the plan should be updated to include any lessons learned.

[Insert procedures for review and updates adopted by PSC.]

3200. Plan Security and Control

To be effective, the PSP needs wide dissemination, but because of the nature of the information contained in the plan, it will also need to be protected. Efforts should be taken by the PSC to control the dissemination of security sensitive information.

[Insert procedures for release of information contained in the plan.]

4000. Port Security Training

Each member of the PSC is responsible for ensuring those members of their organization directly affected by the execution of this plan are trained to an appropriate level to execute their roles in implementing the plan.

5000. Port Security Exercise Program

The Port Security Plan shall be exercised periodically to test the currency and efficiency of the plan's contents. Exercises should include notification, tabletop or full field exercises.

(Exercises may be coordinated as part of other exercises. Objectives may be accomplished by coordination with existing exercise programs.)

[Insert schedule of exercises]

6000. Appendices

(Appendices may be used to segregate classified information. They may also be used to document specific geographic, infrastructure (physical or cyber), port or vessel services, or industry security procedures. Information in this section may be incorporated or referenced as a separate document as appropriate.)

(The titles provided here are examples and may be modified to best fit the documentation decisions made by the PSC.)

6100. (Unclas) Port Security Committee Member Entities, Representatives & Contact Information

6200. (Classified or SSI) Charts and Maps With ID of Port Tenants & Infrastructure

6300. (Classified or SSI) Port Operations and Infrastructure

6400. (Classified or SSI) Risk Based Scenarios

6500. (Classified or SSI) Security Procedures

6510. (Classified or SSI) Risk ranked infrastructure for consequence categories

6520. Setting MARSEC conditions

6530. Actions for MARSEC conditions

6540. Utilization of security resources

6550. Communications Plan

6560. Procedures for Breach of Security

6570. Types of Existing Valid Identification

6600. (Classified or SSI) Dangerous Cargoes for Security Planning.

6700. Agency/Organization Questionnaire

(SAMPLE Port Security Plan)

6100. (Unclas) Port Security Committee Member Entities, Representatives & Contact Information

Name	Agency	Phone, bus. & 24 hour	email

6500. (Classified or SSI) Security Procedures

(A matrix format may be used to document Security Procedures. The following provides an example.)

INITIAL SECURITY PROCEDURES *(EXAMPLE)*

SITUATION	Principle Agency & Contact	Secondary Agency & Contact
Suspicious Container	U.S. Customs	FBI CG
Bomb Threat	FBI	State Local CG
Unauthorized Entry	Local	State
Illegal Immigrants	INS	State

6700. Agency/Organization Questionnaire

[This form is designed to assist in generating information for assessment and plan development.]

Agency/Organizational Questionnaire.

1. What is the name of the agency or organization?

2. What are the roles and responsibilities the agency or organization plays in the maritime or transportation community?

3. Does your agency have any related plans or procedures?

4. What is the jurisdiction or area of responsibility for the agency or organization?

5. Describe the capabilities and resources of the agency or organization.

6. What restrictions would limit the participation of your organization?

7. What method do you use to get participation from your agency in response or mitigation efforts? (E.g. Presidential/governor declaration of emergency).

8. What are the infrastructure requirements that are necessary to keep your agency or organization operating?

Glossary/Definitions
These definitions apply only for the purpose of this plan and do not amend existing legal definitions that may apply in other applications.

(This is not an all inclusive list. Your PSC may decide to eliminate words from this list, to include other words, or modify definitions.)

Awareness – knowledge of port operations, geography, infrastructure and of threats and vulnerability.

Consequence Management – the actions taken after an attack has occurred intended to save lives, reduce injuries, contain the damage, and exercise control over the targeted area.

Infrastructure - the physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private.

Port –the port area and its adjacent waterways, including Marine Transportation System (MTS) infrastructure, especially the ship/port interface in each Captain of the Port Zone.

Port Security Assessments (PSA) – a process that includes threat, criticality and vulnerability assessments to identify a port's vulnerabilities that may be exploited by terrorists and suggests options to eliminate or mitigate.

Port Security Committee (PSC) – provides a framework for communication and coordination to identify threats and reduce vulnerabilities to terrorist actions in and near the Marine Transportation System. The Committee is composed of government agencies, commercial entities and other groups or individuals interested in preserving and improving the security of our shared waterfront areas and Marine Transportation System (MTS).

Port Security Plan (PSP) – a detailed outline of the processes to be put into place to reduce risk in U.S. Ports. It also outlines the process through which a Port Security Committee will assess the vulnerabilities of a port, and develop security procedures to reduce vulnerabilities.

Prevention – the processes and programs in a port that reduce vulnerability.

Risk – 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 – a systematic, analytical process to consider the likelihood that a threat will harm an asset or individuals and to identify actions to reduce the risk and mitigate the consequences on an attack. Risk management principles acknowledge that while risk generally cannot be eliminated, enhancing protection from known or potential threats can reduce it.

Response – any action taken due to a result of an incident.

Threat Assessment – a decision support tool that helps to establish and prioritize security-program requirements, planning, and resource allocations; an assessment that identifies and evaluates each threat on the basis of various factors, including capability, intention, and lethality of an attack.

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 Port Security Committee (PSC). 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 PSC 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 PSC 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 PSC 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*