



# *MARITIME SENTINEL*

## **COAST GUARD STRATEGIC PLAN FOR COMBATING MARITIME TERRORISM**

**MARCH 2006**



## PREFACE

### *From the Commandant of the U.S. Coast Guard*

The United States is fully engaged in the Nation's multi-front war against global terrorism, both at home and abroad. Much has changed since I issued the U.S. Coast Guard Maritime Strategy for Homeland Security 2002. On 21 May, 2003, President Bush described the Coast Guard as America's "shield of freedom." While we have made progress, the homeland remains vulnerable to attack by terrorists who seek to take advantage of our open and democratic society, including exploitation of our maritime borders and Marine Transportation System. As the 9-11 Commission Report noted: "While commercial aviation remains a possible target, opportunities to do harm are as great, or greater, in maritime or surface transportation."

The U.S. Coast Guard has taken on the Commission's and Department's challenges for combating terrorism in the maritime domain. Our strategy for Combating Maritime Terrorism (CMT) includes Ports, Waterways, and Coastal Security (PWCS) activities, as well as Extended Offshore Security Operations (EOSO). *Maritime Sentinel* is the Coast Guard strategy for Combating Maritime Terrorism. It serves as guidance for this critically important mission. This plan preserves the essentials of the aforementioned strategy, including the premium placed on identifying and intercepting threats well before they reach U.S. shores by conducting layered, multi-agency, maritime security operations and by strengthening the port security posture of strategic economic and military ports.

*Maritime Sentinel* continues to recognize our responsibilities and authorities as the lead DHS agency for Maritime Security, the exercising of Federal Maritime Security Coordinator duties by designated Captains of the Port, and our roles and responsibilities in the offshore environment as a supported or supporting commander for Homeland Security or Defense. It aligns with Securing Our Homeland, U.S. Department of Homeland Security Strategic Plan 2004,

responds to the *Secretary's Second Stage Review* imperatives, and incorporates lessons learned over the last three years. It reflects elements of the National Strategy for Maritime Security and its sub-plans, and is responsive to the spirit and letter of the Intelligence Reform and Terrorism Prevention Act of 2004.

*Maritime Sentinel* leverages our military, maritime, multi-mission heritage. It also embraces a threat-based, risk-managed approach. This plan calls for action through the Coast Guard's near term strategy to: (1) Achieve Maritime Domain Awareness; (2) Lead and conduct effective maritime security and response operations; (3) Create and oversee an effective Maritime Security Regime. Implementation of this strategic plan is instrumental in our ability to fulfill our responsibility of countering the full spectrum of threats to the nation's interests within the maritime domain and to maintain the integrity of our nation's maritime border.

Transition and transformation have become watchwords as we unite to assure the security of the country. *Maritime Sentinel* will serve to guide the Coast Guard as we transition to a more proactive force against those who would do us harm, and as we transform toward an integral, yet unique, instrument of national security in the Global War on Terrorism.

Thomas H. Collins  
Admiral, U.S. Coast Guard

# TABLE OF CONTENTS

**PREFACE** ..... **i**

**Table of Contents**..... **1**

**I. Introduction** ..... **2**

    PURPOSE..... 2

    SCOPE..... 3

    PLAN STRUCTURE..... 4

    CONTEXT..... 4

**II. Threat Assessment** ..... **5**

    STRATEGIC ENVIRONMENT..... 5

    MARITIME DOMAIN..... 5

    MARITIME THREATS..... 6

**III. Strategy**..... **7**

    MISSION ..... 7

    STRATEGIC OBJECTIVES ..... 7

*Prevent terrorist attacks, sabotage, espionage and other subversive acts* ..... 7

*Protect* ..... 8

*Minimize Damage and Expedite Recovery* ..... 8

    GUIDING PRINCIPLES..... 8

*Threat-Based Risk-Managed* ..... 9

*Facilitating Commerce* ..... 9

*Active Deterrence* ..... 10

**IV. Courses of Action** ..... **12**

*Achieve Maritime Domain Awareness*..... 12

*Lead and Conduct Maritime Security and Response Operations* ..... 14

*Create and Oversee an Effective Maritime Security Regime*..... 17

**V. Performance Measurement and Improvement, Resourcing, and Key Initiatives**..... **20**

    PERFORMANCE MEASUREMENT..... 20

*Activity Standards*..... 20

*Metrics*..... 21

    PERFORMANCE IMPROVEMENT ..... 22

    RESOURCING ..... 23

    KEY CMT INITIATIVES..... 23

**VI. Summary - The Way Ahead** ..... **25**

**Appendix A: Glossary and Acronyms** ..... **A-1**

**Appendix B: CMT ALIGNMENT TO DHS STRATEGIC PLAN (2004)** ..... **B-1**

**Appendix C: Activities, Standards, and Metrics**..... **C-1**

# I. INTRODUCTION

Sentinel: *A person or special body of persons assigned to provide protection or keep watch over.*

## PURPOSE

*Maritime Sentinel* is the Coast Guard’s Strategy for Combating Maritime Terrorism (CMT). It implements elements of the *National Strategy for Homeland Security*, the *National Strategy for Maritime Security* (and its supporting plans, particularly the *Maritime Operational Threat Response (MOTR) Plan*), and the Maritime Transportation Security Act of 2002. Its direction is consistent with the Secretary’s Second Stage Review.

*Maritime Sentinel* describes the Coast Guard’s efforts to combat maritime terrorism, in terms of Ports, Waterways, and Coastal Security (PWCS) activities and Extended Offshore Security Operations (EOSO). PWCS activities are those that focus mainly on inshore and near-shore regions, leveraging Captain of the Port (COTP) authorities and the Coast Guard’s relationships with State and local authorities, as well as the maritime industry. EOSO generally occur farther seaward and leverage the Coast Guard’s presence and law enforcement competencies that apply throughout the full expanse of the maritime domain. Figure 1 illustrates *Maritime Sentinel*’s place in a greater hierarchy of related plans.

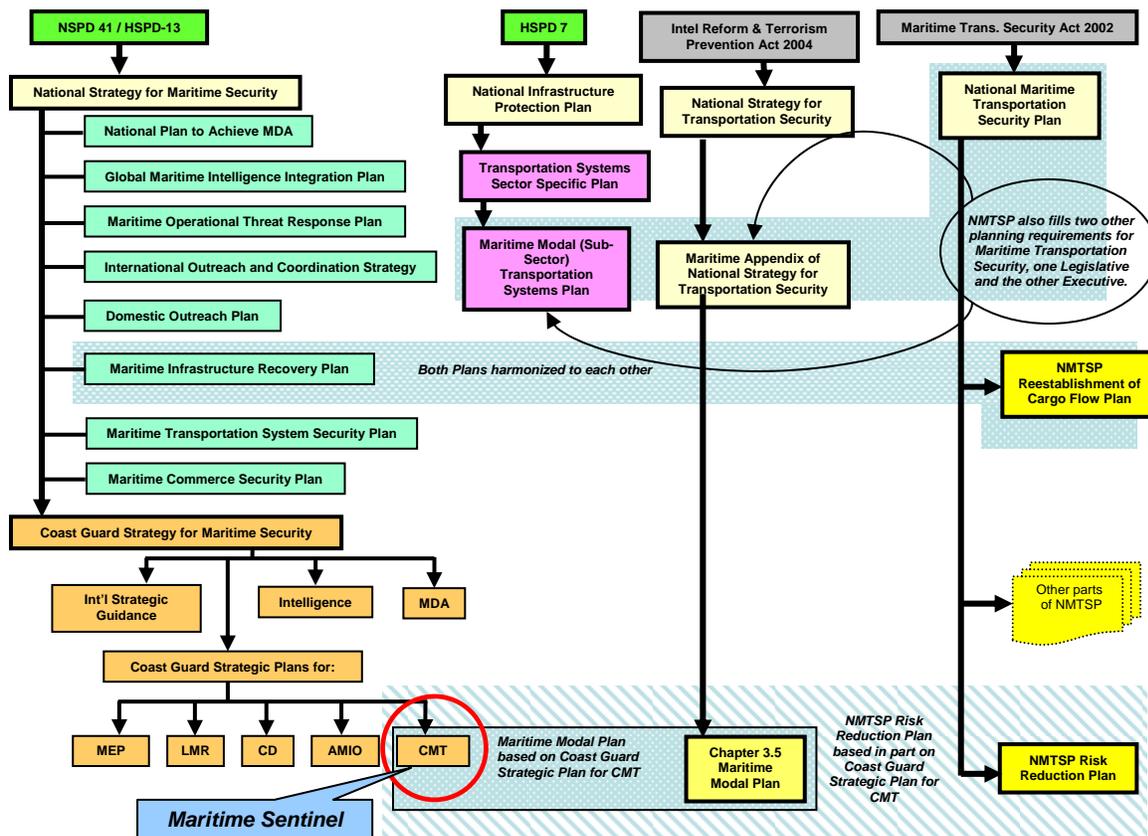


Figure 1  
Relationships of Maritime Strategies and Plans

*Maritime Sentinel* underscores the need for preparedness of the Coast Guard. It also reinforces the involvement of other maritime stakeholders (i.e., international, other Federal, state and local partners, and the maritime industry) necessary to combat maritime terrorism. This document sets forth the mission objectives, operational activities, and standards and measures for combating terrorism, as well as identifying key CMT initiatives.

## SCOPE

*Maritime Sentinel* applies to the Coast Guard's CMT mission, including both EOSO and PWCS activities, as described herein.

**Mission:** CMT is the post-9/11 descriptor given to the Coast Guard's mission to protect the U.S. Maritime Domain and U.S. Marine Transportation System (MTS); prevent terrorist attacks, sabotage, espionage, or subversive acts; and respond to and recover from attacks that do occur. CMT includes the employment of awareness activities, antiterrorism and counterterrorism operations, and the establishment and oversight of a maritime security regime. The CMT mission requires a high degree of preparedness on the part of the Coast Guard.

PWCS builds on the Coast Guard's legacy port security mission focused on defeating sabotage, espionage and other subversive acts. The authority for this legacy port security mission is primarily derived from the Espionage Act of 1917, the Magnuson Act of 1950 and Executive Order 10173. PWCS leverages decades of port security experience, as well as extensive Coast Guard authorities, competencies, capabilities, and partnerships to provide a robust security framework in the ports, coastal approaches.

EOSO relies on the Coast Guard's persistent presence and operational capability in the offshore waters of the Atlantic and Pacific Oceans and the Caribbean Sea. National strategy compels a layered approach to maritime security structured to identify and resolve threats as far as possible from U.S. shores. EOSO activities are integral to that construct. Cutters and aircraft conducting maritime security missions offshore including drug interdiction, migrant interdiction, defense readiness, and protection of U. S. maritime resources contribute to domain awareness and are operational means through which the Coast Guard supports an agile national offshore Maritime Operational Threat Response (MOTR) capability.

*Maritime Sentinel* provides a framework to guide the conduct of the CMT mission. It guides near-term (2-5 years) CMT growth and development in these areas and builds on previous strategies, including the Coast Guard's Maritime Strategy for Homeland Security (originally published in December, 2002). It aligns CMT objectives, metrics and supporting initiatives to the 2004 Department of Homeland Security Strategic Plan.

## PLAN STRUCTURE

Sections II through V discuss:

- **Threat Assessment:** Outline the strategic threat environment and the inherent challenges of preventing terrorist/subversive acts in the maritime domain, and provide an overview of the maritime threats we face from which to base investment and policy decisions, as well as to conduct security operations and establish a maritime security regime.
- **Strategy:** Outline the strategic mission and objectives for clarity of purpose across key Coast Guard stakeholders.
- **Courses of Action:** Outline the guiding operational concepts the Coast Guard will employ, the courses of action embarked upon to accomplish CMT objectives, as well as the core capabilities needed for successful mission execution.
- **Performance Measurement and Improvement, Resourcing, and Key Initiatives:** Outline the CMT performance measurement framework, the analytical and systematic tools we will employ to enhance performance, and the key initiatives and milestones the Coast Guard will pursue in the near term (2-5 years).

## CONTEXT

As the initial version of *Maritime Sentinel*, version 1.0 is to be used as a baseline or starting point. Consequently, the CMT activities, standards, and metrics contained in Appendix C reflect today's CMT mission expectations, rather than a desired end state for that mission. Standards for the desired end or future state, as well as a plan to reach that state, will be contained in version 2.0 and subsequent versions of *Maritime Sentinel*.

Additionally, the standards contained in *Maritime Sentinel* (version 1.0) are based mainly on the collective best professional judgment of various subject matter experts on the Coast Guard's Headquarters and Area staffs. Version 2.0 and subsequent versions will be based, as much as possible, on greater analysis, including operations research and several detailed studies (e.g., deterrence studies).

## II. THREAT ASSESSMENT

### STRATEGIC ENVIRONMENT

As stated in the National Strategy for Maritime Security, “Complexity and ambiguity are hallmarks of today’s security environment, especially in the maritime domain.” The maritime domain in particular presents not only a medium by which these threats can move, but offers a broad array of potential targets that fit the terrorists’ operational objectives...” Defeating the threat of the widely dispersed terrorist networks that present an immediate danger to U.S. national security interests at home and abroad remains our foremost objective.”<sup>1</sup>

### MARITIME DOMAIN

Distinct from other domains (e.g., air and land), the maritime domain has relatively few access barriers and provides an expansive pathway for a wide spectrum of threats. Terrorists recognize this particular vulnerability as well as the extraordinary value of critical infrastructure, key assets, and population centers concentrated along the nation’s coasts and waterways.

The United States is necessarily reliant on the oceans as global thoroughfares that sustain our national prosperity and as the very avenues of our freedom. The offshore maritime domain is an ‘open system’ characterized by the continuous intermingling of many vessels of dissimilar type and registry, bound for various ultimate destinations, carrying cargos of all kinds for international customers who are not linked directly to the vessels, maritime agents, or Flag States of registry facilitating the movement of their goods. Sharing the domain with merchant ships are sizeable foreign and domestic commercial fishing fleets that, along with research and many types of work vessels, conduct at-sea operations as well as interstate and international voyages. The open nature of the offshore environment is at once the source of efficiency and vulnerability in the global maritime domain. The offshore waters of the Atlantic and Pacific oceans and the Caribbean Sea are regions in which the Coast Guard routinely operates and through which most international maritime threats must pass in order to successfully reach our homeland.

Approximately 95% of the United States’ overseas trade passes through its ports, accounting for two billion tons and almost \$800 billion of domestic and international freight each year. Our coastal waterways support approximately 110,000 commercial fishing vessels contributing \$110 billion to state economies each year. Additionally, more than 141 million U.S. citizens – over half the population – live within 50 miles of the coast. By 2025, that is expected to grow to 75 percent of the population. The coastlines of the U.S. host approximately 181 million tourists each year and support over 28 million jobs.

In addition to coastal waterways, there are nearly 12,000 miles of commercially active inland and intracoastal waterways in the United States. These waterways are supported

---

<sup>1</sup> The National Strategy for Maritime Security, September 2005

by locks and dams with a replacement value of over \$125 billion. Approximately 1,800 river terminals are distributed across 21 states, with 59% servicing dry bulk cargoes and 27% servicing liquid bulk cargoes. Approximately 22,000 dry cargo barges and 3,000 tank barges service these terminals. The nation's inland waterways cargo transportation services support nearly 800,000 jobs. Inland waterways carry approximately 15% of the total freight transported in the U.S., with the annual value of goods exchanged between states using water transportation exceeding \$100 billion. Total inland waterway freight is expected to increase by 1.3% annually, to more than 836 million tons by 2020.

### **MARITIME THREATS**

The National Strategy for Maritime Security categorizes maritime threats into nation-state threats; terrorist threats; transnational criminal and piracy threats; environmental destruction; and illegal seaborne immigration. The Coast Guard's CMT mission focuses on terrorist threats and the threats of sabotage, espionage and other subversive acts.

The volume of commercial shipping across our ocean approaches presents unique risks and implications for maritime security. Additional challenges derive from the complexities of shared use of oceans and waterways, long-standing international respect for freedom of navigation, and transnational seams between our air, land, sea, and subsurface borders. Adversaries may seek to exploit the maritime domain in an effort to employ, as operational enablers, anonymity and relative obscurity against a vast and teeming backdrop. The potential for commercial vessels to be used to convey terrorists, transnational criminals, or their wares, including weapons of mass destruction, is a real and persistent threat that can be discovered at any time and become actionable at any point along a vessel's transit to the U.S.

#### **Terrorist Threats in the Maritime Domain**

Terrorists can develop effective attack capabilities relatively quickly using a variety of platforms, including explosives-laden suicide boats and light aircraft; merchant and cruise ships as kinetic weapons to ram another vessel, warship, port facility, or offshore platform; commercial vessels as launch platforms for missile attacks; underwater swimmers to infiltrate ports; and unmanned underwater explosive delivery vehicles. Mines are also an effective weapon because they are low-cost, readily available, easily deployed, difficult to counter, and require minimal training. Terrorists can also take advantage of a vessel's legitimate cargo, such as chemicals, petroleum, or liquefied natural gas, as the explosive component of an attack. Vessels can be used to transport powerful conventional explosives or WMD for detonation in a port or alongside an offshore facility.

Terrorist Threats – National Strategy for Maritime Security, September 2005

### III. STRATEGY

#### MISSION

The Coast Guard CMT mission is to protect the U.S. Maritime Domain and U.S. Marine Transportation System (MTS); prevent terrorist attacks, sabotage, espionage, or subversive acts; and respond to and recover from those that do occur. CMT includes the employment of awareness activities; counterterrorism, antiterrorism, and response operations; and the establishment and oversight of a maritime security regime. The measure of success for the Coast Guard's CMT mission is the reduction of the risk due to terrorism, sabotage, espionage, and other subversive acts in the maritime domain.

To achieve the mission, the Coast Guard will pursue the below strategic objectives.

#### STRATEGIC OBJECTIVES

A strategic objective describes the end state which can be achieved through successful execution of supporting tasks and activities. The strategic objectives for the CMT mission are to:

- Prevent and respond to a terrorist / subversive attack within the maritime domain.
- Reduce America's vulnerabilities to terrorist/subversive acts.
- Protect U.S. population centers, critical infrastructure (including but not limited to the MTS), maritime borders, ports, waterways, coastal approaches, offshore regions, and the boundaries and seams between them.
- Minimize the damage to and expedite recovery from terrorists/subversive attacks that may occur within the maritime domain.

Each objective is aligned within the construct of the Department of Homeland Security (DHS) strategic goals outlined in the 2004 DHS Strategic Plan, as follows:

#### **Prevent terrorist attacks, sabotage, espionage and other subversive acts**

##### **Detect, deter, interdict and defeat terrorist attacks, sabotage, espionage and other subversive acts in the Maritime Domain, and prevent its unlawful exploitation for those purposes**

Achieving this objective requires a level of maritime security operations--especially detection, deterrence and effective end-game prosecution, including counterterrorism capabilities--that must be enduring, sustainable, and flexible in application. Coast Guard forces must be equipped and arrayed to conduct layered maritime security operations that detect and resolve threats as far from U.S. shores as possible. Persistent surveillance and tracking, and increased partnerships and interagency coordination among multiple civil, military, law enforcement, and private sector organizations will serve to mitigate security threats within the Maritime Domain. In addition, threats will be mitigated through regulatory and law enforcement initiatives.

## Protect

### **Protect maritime-related population centers, critical infrastructure, key resources, transportation systems, borders, harbors, ports, and coastal approaches in the maritime domain**

The Coast Guard will conduct operations, in conjunction with Federal departments, state and local agencies, and other maritime stakeholders, in ports, waterways and coastal/offshore areas of the United States to protect and safeguard high-risk waterfront facilities, infrastructures, vessels, harbors, or waters from terrorism and other subversive acts. The Coast Guard will continually utilize threat, vulnerability, and criticality assessments and real-time, comprehensive domain awareness of maritime approaches, the coastline, ports and inland waterways, navigation and telecommunication infrastructure, and other critical infrastructure to allocate resources.

## Minimize Damage and Expedite Recovery

### **Minimize damage and expedite recovery from attacks within the maritime domain**

To accomplish this, the Coast Guard will align its response plans with the single all-discipline, all-hazard National Response Plan. The Coast Guard will also work with other Federal, state, local, and nongovernmental security and safety organizations to integrate response activities in the maritime domain.

## GUIDING PRINCIPLES

In pursuing these Strategic Objectives, the Coast Guard is guided by the following principles. They are overarching concepts that will inform the development and implementation of activities across all strategic objectives (Prevent, Protect, Respond, and Recover).

## Layered Security

The Coast Guard fully embraces the concept of defense-in-depth, and this concept is evident in all three Courses of Action, to be discussed in Section IV. The Coast Guard operates in every maritime layer in anticipation of, or in response to, changing threats, adversary tactics, and operational conditions. The *National Strategy for Maritime Security* emphasizes the need to patrol, monitor, and exert unambiguous control over our maritime borders and maritime approaches. It goes on to emphasize that *at-sea presence* reassures U.S. citizens, *deters* adversaries and lawbreakers, provides better mobile surveillance coverage, adds to the warning time, allows seizing the initiative to influence events at a distance, and facilitates the capability to surprise and engage adversaries well before they can cause harm to the United States. During the course of routine operations, as well as specified security missions, Coast Guard cutters and aircraft operate in the offshore waters of the Atlantic and Pacific Oceans, and in the Caribbean Sea, to provide MDA, CMT command and control and capability to respond to maritime threats. Through such initiatives as the Integrated Deepwater System (IDS) acquisition, the Coast

Guard is enhancing its capability to keep potential adversaries off balance through an effective defense of U.S. territory and, when necessary, by projecting operational presence far to seaward.

Maritime Security Regime initiatives seek to unify regional and global efforts to render the maritime domain inhospitable to terrorism and related illegal activities. Chartered interagency and international frameworks are being developed to share security information; form and exercise international and regional security agreements; conduct cooperative operations; and enforce regulations consistently and collaboratively across transnational seams. Maritime Security Regimes support a layered security approach by enhancing detection and resolution of potential maritime threats at their ports of origin and by increasing capabilities to illuminate and interdict threats in transit anywhere within the global maritime transportation system.

*Maritime Sentinel*, version 1.0 reflects today's best effort to provide for a layered security. The standards which will be contained in *Maritime Sentinel*, version 2.0 will drive toward an end state providing even greater defense-in-depth.

### **Threat-Based Risk-Managed**

The U.S. Maritime Domain is too expansive to protect with dedicated denial forces. Resources, manpower, and equipment are too limited to protect everything all of the time. Terrorists understand these limitations and seek to take advantage of them. CMT success will therefore hinge, in part, on a set of threat-based, risk-managed activities which focus efforts and resources on the Maritime Critical Infrastructure and Key Assets (MCI / KA) facing the highest maritime risks.

### **Leverage Intelligence Information to Guide Operations**

An active, seamless, layered defense relies on early warning of emerging threats in order to quickly deploy and execute a decisive response. The Coast Guard is a key member in a growing National maritime intelligence enterprise and must continually strive to adapt and integrate all available information to maximize the timeliness and fidelity of its common intelligence picture (CIP). The CIP informs our understanding of risks and active threats within the maritime domain. This intelligence is used, in turn, as a basis for structuring preventative activities to reduce security risks and to prompt decisive protective operations as needed to address threats. Intelligence is therefore integral to the design of maritime security plans and the conduct of activities that achieve maximum operational impact.

### **Facilitating Commerce**

Disrupting the U.S. economy is a primary terrorist goal. Therefore the provision of security must be accomplished while preserving the freedom of the maritime domain for legitimate pursuits. It is necessary to establish effective partnerships and coalitions with international, Federal, state, local and tribal agencies, as well as the private sector and academia.

## Active Deterrence

National strategies related to Homeland Security place a premium on preventing terrorist attacks and operations. While Coast Guard law enforcement strategy has relied on principles of deterrence, their effects are not well understood with respect to terrorism. The Coast Guard, in cooperation with other department stakeholders, is actively studying and building models to assess the deterrent effect of enforcement presence and maritime security activities.

The Coast Guard's EOSO and PWCS activities are based in part on deterrence by denial. Coast Guard forces must prevent or disrupt terrorists from achieving their attack objectives. Disrupting terrorists' pre-strike activities, such as surveillance and planning, can effectively delay terrorist actions or cause terrorists to take additional steps or measures, which may provide greater opportunities for detection and interdiction by Coast Guard or other law enforcement agencies.

The Coast Guard's layered, threat-based, risk-managed approach seeks to resolve threats at the optimal operational juncture:

- Those discovered with sufficient warning aided by collaborative international partnerships at departure ports;
- Those best resolved at a standoff distance from U. S. interests by interdicting them offshore; and
- Those that can be suitably addressed upon arrival through Coast Guard and collaborative interagency security actions in U.S. ports and coastal waters.

“...Defenses cannot achieve perfect safety. They make targets harder to attack successfully, and they deter attacks by making capture more likely. Just increasing the attackers' odds of failure may make the difference between a plan attempted, or a plan discarded. The enemy also may have to develop more elaborate plan, thereby increasing the danger of exposure or defeat. “

-- The 9/11 Commission Report

Figure 2 is a graphic depiction of layered security provided by the integration of EOSO and PWCS activities.



Figure 2  
Layered Security

## IV. COURSES OF ACTION

In order to accomplish the CMT Strategic Objectives, the Coast Guard has selected a three-pronged approach related to EOSO and PWCS activities.

Achieve Maritime Domain Awareness (MDA)

Lead and Conduct Effective Maritime Security and Response Operations

Create and Oversee an Effective Maritime Security Regime

### **Achieve Maritime Domain Awareness**

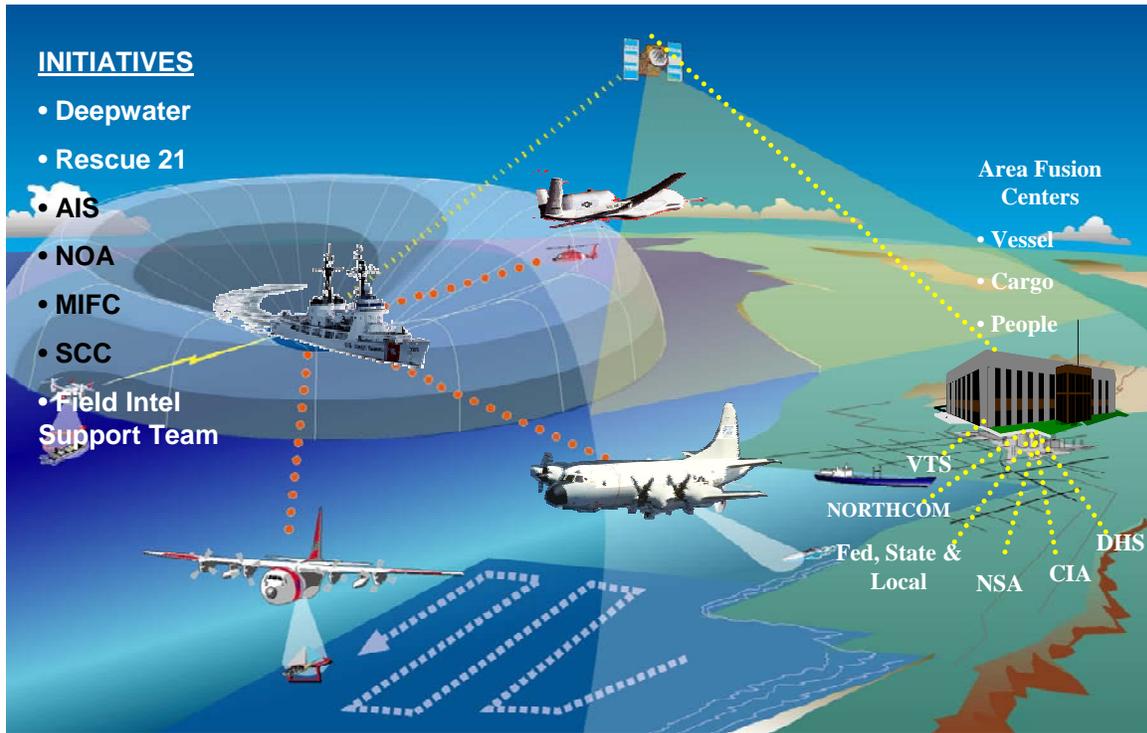
Maritime Domain Awareness (MDA) is the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States. It is a core enabler for all CG missions.

Attaining and sustaining an effective understanding of the maritime domain requires: (1) the collection, fusion, analysis, and dissemination of prioritized categories of data, information, and intelligence to decision makers; and (2) the application of knowledge regarding the full spectrum of maritime threats. A large amount of information and intelligence supporting MDA is already being collected, analyzed, and disseminated from a wide variety of sources both within and outside of the Coast Guard.

A key component of MDA includes the continual monitoring and evaluation of information and intelligence regarding oceanic shipping by Coast Guard and partner agencies. This process seeks to accurately and expeditiously identify in-transit threats and becomes more focused when the intent to call on a U.S. port is communicated through the mandatory 96-hour advance Notice of Arrival (NOA). Based on NOA information, collaborative and sophisticated analyses of crew and cargo manifests; ship and corporate associations; and transit history are performed. When cross-correlated with threat intelligence, the result is an aggregate level of perceived threat represented by a vessel as it proceeds toward arrival at a U.S. port. In most cases a threat-based, risk-managed approach classifies threats as able to be adequately and efficiently addressed through PWCS strategies employed near or upon arrival at the destination port. Yet, the case analysis may suggest a degree of suspicion or risk of harmful intent relative to a specific vessel, its crew, passengers, or cargo of such significance that the vessel not be permitted to approach the coastal or port environment until further investigated. The intelligence in such cases may lead to a conclusion that the optimal MOTR involves boarding the vessel well offshore—far from our ports, population centers, and elements of critical infrastructure—to confirm or refute the cause of suspicion.

Figure 3 is a graphic representation of the C4ISR and other capabilities and contributors to achieving Maritime Domain Awareness.

Figure 3  
 Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance (C4ISR)



MDA activities include but are not limited to the following:

Monitor Vessels and Other Craft in the Global Maritime Environment: Vessels and other craft are monitored by various means and displayed on a Common Operational Picture (COP) to facilitate operational decision-making or other actions.

Monitor People and Organizations in the Global Maritime Environment: Crew and passenger lists are screened and compared with various databases to facilitate sorting and operational decision-making.

Monitor Cargo in the Global in the Maritime Environment: The movement of vessels carrying cargoes designated by the National Targeting Center, as well as Certain Dangerous Cargoes (CDCs) is monitored as they transit into and out of coastal ports, as well as within the nation's inland river system.

Monitor Identified Areas of Interest in the Global Maritime Environment: This activity involves the monitoring of certain designated geographic areas, based on either permanent interest or temporary interest (e.g., during NSSEs).

Access and Maintain Data on Infrastructure, Facilities, Vessels, Cargo, and People: Provide national maritime critical infrastructure / key asset (MCI / KA) information into enterprise Global Information System (GIS) data base for Militarily and Economic Strategic (MES) ports.

Collect, Fuse, Analyze, and Disseminate Information and Intelligence: These are classic intelligence processes designed to support strategic, operational, and tactical decision-making. These activities are carried out at the national level (e.g., Coast Guard Intelligence Coordination Center), at the operational Level (e.g., Area MIFCs), and at the field level (e.g., Field Intelligence Support Teams).

### **Lead and Conduct Maritime Security and Response Operations**

The Coast Guard has extensive experience and expertise in maritime security and response operations and risk management. By exploiting knowledge of maritime conditions, Coast Guard forces, supported by other military and interagency forces where appropriate, will conduct maritime security and response operations in the Global Maritime Domain.

Coast Guard-wide guidance for the mix of operations to combat maritime terrorism and their execution has been promulgated in an Operation Neptune Shield (ONS) operations order (OPORD) and other directives. The operational activity standards set forth in that order are based upon current capabilities and our current understanding of maritime threat and risk, as well as effective mitigation. The order and its standards are modified periodically as capabilities increase, and/or as our understanding of maritime risk matures. Operational activities include but are not limited to the following:

**Conduct Waterborne, Shoreside, and Aerial Patrols:** These activities both within ports and along waterways, as well as offshore are conducted to project varied and unpredictable credible presence and increase awareness in order to detect, deter, interdict, and defeat the surveillance, planning, and actions of terrorists or subversives in the Maritime Domain.

**Conduct Security Boardings:** Conduct security boardings<sup>2</sup> and associated activities, including:

**Security Boardings of High Interest Vessels (HIVs)/non-HIVs:** Examine a vessel's cargo documentation and persons on board to assess if vessel should be permitted to enter port and if additional security measures are warranted (see Positive Control Measures).

**Positive Control Measures:** The stationing of armed boarding team members at key locations onboard a vessel, ensuring the vessel remains under control of appropriate authorities during its transit of key port areas in order to prevent its use as a kinetic weapon.

**Security Boardings of Small Vessels (<300 GT):** Conduct boardings of vessels that could be used to smuggle weapons or people, or used as a vessel-borne improvised explosive device (VBIED), or USS Cole-style attack to threaten MCI/KA.

**Security Boardings of Suspect Vessels:** Investigate vessels for which there are reasonable grounds to suspect involvement in terrorist or subversive activity; preempt attack; interdict terrorists before they can threaten U.S. interests.

**Escort Vessels:** Includes the provision of armed Coast Guard assets (waterborne and/or aerial) to accompany selected vessels (e.g., HIVs, CDC Vessels, HVUs, HCPVs) during transits, especially during transits of key port areas. The purpose is to provide an armed deterrent presence for protection of selected vessels from surface attacks and of key port areas from the effects of successful attacks by other vessels.

**Enforce Fixed Security Zones:** Establish, monitor, and enforce security zones around fixed MCI/KA, both within ports and offshore. The purpose is to provide armed deterrent presence and external protection for MCI / KA from surface or underwater attacks.

**Establish Offshore Presence:** The Coast Guard always maintains a persistent presence of large cutters in the Atlantic, Pacific, and Caribbean in order to conduct counterdrug (CD), alien migrant interdiction operations (AMIO), fisheries enforcement, and general law enforcement operations. These multi-mission capable assets may be diverted, and/or additional assets may be dispatched to these offshore regions and beyond, in support of the CMT mission. The purpose of such offshore presence is to provide additional MDA, command and control, and boarding / interdiction platforms capable of responding to maritime threats and/or intelligence cueing. The desired result is to reduce risk by enabling the investigation and / or interdiction of serious security threats at greater ranges

---

<sup>2</sup> Security Boarding: An examination by an armed boarding team of a vessel (including the cargo, documentation, and persons on board), including vessels of interest (VOI), designated by the COTP or District / Area Commander, arriving or departing a U.S. port or offshore, to deter acts of terrorism and/or transportation security incidents. (Source: ALCOAST 506 / 05)

from U.S. shores. Such offshore presence enhances the responsiveness of Coast Guard interdiction efforts, in accordance with the Maritime Operational Threat Response (MOTR) Plan, which directs DHS to plan for “the conduct of offshore cordon and search procedures for vessels prior to entry into U.S. ports.” Actions taken offshore to resolve suspicion generated by intelligence data regarding vessels bound for U.S. ports must respect the balance between commerce and security, and conform to domestic and international law.

**Conduct Surge Operations:** Conduct short-duration increases in Coast Guard presence and activities in order to decrease predictability and disrupt terrorist surveillance, planning, and execution activities.

**Investigate Anomalies:** Investigate reports of suspicious or unusual activities in and around U.S. ports and waterways, which may be received via MDA activities, the public, maritime industry, or other sources.

**Control Port Access, Activity and Movement.** As warranted by security and safety circumstances, COTPs may require additional risk based security measures of the maritime industry or specific segment thereof. COTPs exercise their statutory authority to ensure ports, waterways and coastal security and/or mitigate damages from a terrorist act through actions that include closing ports, suspending facility operations, directing the movement of vessels, etc.

**Deploy Specialized Antiterrorism (AT) and Counterterrorism (CT) Assets:** Deploy specialized maritime security units with defensive assets / capabilities in order to prevent attacks and protect selected targets in high risk scenarios. Deploy specialized maritime security units with offensive assets / capabilities to neutralize imminent threats. Examples of specialized maritime security units include Maritime Safety and Security Teams (MSSTs) (AT) and the Enhanced MSST / Maritime Security Response Team (EMSST / MSRT) (CT). Such assets are not organic at every port. Deployment of such specialized assets are often, but not exclusively executed as part of the USCG’s support to National Special Security Events (NSSEs) and other Special Security Events.

**Conduct Military Outload (MOL) Security Support:** Provide Security Support to MOL for operations involving loading / unloading of military cargo or ammunition in support of actual or potential combat operations.

**Support Execution of National Response Plan (NRP):** During incident response / recovery operations, support pertinent Emergency Support Functions (ESFs) under the National Response Plan (NRP). Assist interagency response to a successful terrorist attack to mitigate impact, and facilitate recovery of the MTS.

**Fulfill Role as Federal Maritime Security Coordinator:** Coordinate antiterrorism efforts with appropriate stakeholders. Oversee implementation of Area Maritime Security Plans. In collaboration with local maritime industry, restore flow of commerce in COTP zone.

**Support Incident Command Posts:** For significant terrorist incidents or events, using Incident Management Assist Team (IMAT) personnel, augment COTP forces in the staffing of local Incident Command Posts / Unified Command Posts.

**Support Joint Field Offices (JFOs):** For significant terrorist incidents or events, using Incident Management Assist Team (IMAT) personnel, augment other USCG forces in the staffing of the JFO.

### **Create and Oversee an Effective Maritime Security Regime**

The Coast Guard will facilitate a Maritime Security Regime as a collaborative framework of domestic and international partnerships and regulatory initiatives in which counterparts collectively engage on shared maritime security interests; share information; conduct cooperative operations; and develop and exercise mutual plans and security agreements. Examples that incorporate an integrated and layered approach to security management with multiple means of prevention, protection, and response include, but are not limited to: establishing national and international maritime standards, regulations, and enforcement protocols with relevant and bilateral/multilateral security agreements and treaties; conducting international visits and participating in security forums; establishing common information sharing protocols; and, developing security plans, encouraging and conducting drills, exercises, and professional exchanges.

Regulatory, security compliance assessment, and engagement activities are designed to leverage the capabilities of industry, the public, and international partners. The Maritime Transportation Security Act (MTSA) of 2002, which enacted 46 USC Chapter 701, and the International Ship and Port Facility Security (ISPS) Code are keys to the regulatory aspects of a Maritime Security Regime. The Coast Guard developed and promulgated regulations to affect certain provisions of the Maritime Transportation Security Act of 2002 (MTSA 2002). These provisions were those that involved state, local and maritime industry stakeholders. Internationally, the Coast Guard, within the International Maritime Organization (IMO), led the maritime nations in the development and adoption of the International Ship and Port Facility Code (ISPS). Activities under these broad initiatives include:

**Review, Approve, and Enforce Compliance with Domestic Vessel, Facility and Outer Continental Shelf (OCS) Facility Security Plans:** 85% of the nation's critical infrastructure and key assets are privately owned. MTSA regulations stipulate that MTSA-regulated vessels, facilities, and OCS facilities shall develop and submit security plans, and once approved, operate in accordance with them. These are the first in a family of plans which contain security measures for each Maritime Security (MARSEC) level (1, 2, and 3). Contained in these plans are security measures that vessels, facilities, and OCS facilities will take, such as, access control, restricted areas, handling cargo, and monitoring. Additionally, vessels, facilities, and OCS facilities are required to conduct security assessments that generally describe the vessel, facility or OCS facility and identify its vulnerabilities. Periodically, vessels, facilities, and OCS facilities will be

checked for compliance with their plans. Appropriately investigate and address non-compliance. Additionally, their plans will be routinely exercised and evaluated in an effort to improve security.

**Enforce Foreign Flag Vessel Compliance with International Ship and Port Facility Security (ISPS) Code - Implement and Monitor Port State Control Measures:** Vessels of countries signatory to ISPS Code are required to possess and operate in accordance with their ship security plans. These plans were submitted to, and reviewed and approved by the flag state. As part of its security compliance measures, the Coast Guard boarded every foreign flag vessel upon its first arrival after the July 1, 2004 effective date of the ISPS Code. Coast Guard boarding team members verified the existence of the vessel's security plan and assessed its compliance with the plan. Appropriately investigate and address non-compliance. Continued compliance will be enforced during subsequent and random boarding of the vessels.

**Execute International Port Security Program:** The Coast Guard is required to assess the effectiveness of antiterrorism measures maintained at foreign ports served by U.S. flag vessels, from which foreign flag vessels depart on a voyage to the U.S., and any other foreign ports deemed by the DHS Secretary to pose a security risk to international maritime commerce. To accomplish this, the Coast Guard is conducting country visits. Regionally assigned International Port Security Liaison Officers (IPSLOs) facilitate these country visits. An overall assessment of a country's antiterrorism measures starts with an information exchange and ends with visits to select ports. This process allows the Coast Guard to project a three-year cycle to visit 135 nations.

**Lead Outreach/Partnership Activities:** Chair and Lead Area Maritime Security Committees (AMSCs). 46 USC 70103 establishes the Federal Maritime Security Coordinator (FMSC) role for the Coast Guard. Acting in the capacity of FMSC, the Coast Guard chairs each of the regional AMSCs. The membership of the AMSCs includes other Federal, territorial, tribal, state, and local government representatives; other Federal, state, and local public safety, crisis management and emergency response agencies; other Federal, state and local law enforcement and security agencies; maritime industry; and other port stakeholders. The responsibilities of the AMSCs cover the entire spectrum of security activities: awareness, prevention, preparedness, response, and recovery. The dynamic interactions of the members produce tremendous dividends in the form of expedient communications, coordinated prevention, greater preparedness and more effective response and recovery. AMSCs are specifically required to ensure that a risk-based Area Maritime Security (AMS) Assessment is performed for their area of responsibility. The AMS Assessment addresses, among other things, the identification of MCI/KA, the identification and potential of germane threats, vulnerabilities, and consequences.

**Review, Approve, and Exercise Area Maritime Security Plans (AMSPs):** These plans are major products of the Area Maritime Security Committees (AMSCs) and represent the second level of plans within the "family" of MTSA security plans. They must be based on the AMS Assessments and must be consistent with the National Maritime

Transportation Security Plan (NMTSP) discussed below. AMSPs have been drafted and reviewed by the Area Maritime Security Committees (AMSCs) for each COTP Zone. Some important features of an AMSP are the discussion of a port's MARSEC Level 1, 2, and 3 security measures, and procedures for reporting transportation security incidents (TSIs). AMSPs are exercised and evaluated annually.

**Prepare and Exercise National Maritime Transportation Security Plan (NMTSP):**

The NMTSP is the overarching plan in the "family" of MTSA security plans. This plan aligns with national strategy documents such as the National Strategy for Homeland Security, and NSPD 41/HSPD 13's suite of plans including the capstone, National Strategy for Maritime Security.

**Execute and Monitor the Special Interest Vessel (SIV) Program:** The SIV program is the element of the Presidentially-directed U.S. Port Security Program that controls and monitors the entry of vessels that bear the flag of certain States into U.S. ports, internal waters and territorial seas (ref: Presidential Decision Directive – 40 (PDD-40)). The program is applicable to foreign flag commercial cargo vessels, passenger, fishing and fisheries support vessels and private yachts from countries that have been identified by the Administration as potential threats to national security while in U.S. waters.

## V. PERFORMANCE MEASUREMENT AND IMPROVEMENT, RESOURCING, AND KEY INITIATIVES

The Coast Guard will manage its Combating Maritime Terrorism mission in accordance with Executive and Congressional guidance, particularly with respect to risk management imperatives. In close cooperation with the Department, the Intelligence Community, national and international partners, the Coast Guard will routinely:

- Assess current and forecast threats, vulnerabilities and consequences,
- Identify high-risk scenarios,
- Develop risk-mitigation alternatives,
- Select those alternatives having the greatest expected risk reduction value,
- Implement those measures,
- Obtain/allocate resources to maximize risk reduction value,
- Monitor performance in relation to expectations, and
- Adapt consistent measures with observations.

Program performance will be tracked with respect to expected risk mitigation outcome, readiness, and return-on-investment. The Coast Guard will rapidly adapt every aspect of its risk management practices as this critically important discipline evolves. In particular, the Coast Guard will strive to integrate strategic risk assessment information in geospatial, temporal risk maps; to harness the best analytic and modeling tools to develop, deploy and monitor effective interventions. Additionally, the Coast Guard will exploit red teaming, using subject matter experts to role-play adversaries, and exercising real world experience for maximum learning value. The Coast Guard will continue constructive engagements with the Department of Homeland Security, GAO and others to accelerate risk management practice progress.

The Coast Guard will assess its performance through a series of outcome, output and activity measures. A risk-based outcome measure is under active development and will establish a measurement baseline for FY 2006. Current generation performance measures and standards are developed at the strategic (national) level to evaluate the effectiveness of the CMT mission in meeting outcome goals per Appendix C (classified).

### PERFORMANCE MEASUREMENT

#### Activity Standards

The Coast Guard actively manages the performance of its CMT mission by establishing standards for activities (outputs) that impact mission desired outcomes. Operational standards are based on the appropriate level of activity desired to meet strategic objectives. These will be the subject of regular review and will be revised as appropriate to respond to identified or changing threats and operating conditions. Additional standards are drawn from statutory requirements (e.g., MTSA) that set levels of expected Coast Guard performance.

Appendix C details the CMT mission activity standards. Appendix C also highlights linkages between specific USCG CMT activities / standards with DHS Strategic Goals and Second Stage Review Imperatives, as well as with the National Strategy for Maritime Security.

It is important to note that the activity Standards listed within Appendix C, Table 2, which addresses Security and Response Operations, reflect MARSEC 1 level operations. In accordance with the Neptune Shield OPOD, MARSEC 1 activities apply nationwide (i.e., in all ports / locations). However, the OPOD recognizes that resource limitations may sometimes preclude meeting all MARSEC 1 requirements at all locations. In such instances, the OPOD directs the use of Risk Based Decision Making and that Military and Economic Strategic (MES) ports are given priority consideration.

**Metrics**

Figure 4 contains key terms of reference related to the metrics which follow.

<b>Types of measure:</b>	
Output	Product or service desired by a customer that is the immediate result of an activity (e.g., numbers of boardings, etc.)
Outcome	Public benefit the Coast Guard seeks to achieve or influence
<b>Tier:</b>	
Tier I	Reported outside the Coast Guard via the annual performance reporting system
Tier II	Measures designed to link CMT activities to the programs outcome.
Tier III	Measures designed for monitoring internal program performance and are not normally reported outside of the CG.

Figure 4 - Metric Terms of Reference

**Tier I Measures:** The Coast Guard will have a single Tier I CMT Outcome measure that is reported annually in accordance with the Government Performance and Results Act (GPRA) and other executive branch guidance. It will be a risk-based measure that through an established and regular process will require principal CMT program stakeholders to assess the level of maritime risk at a national level. This assessment will include consideration of threats, vulnerabilities and consequences. Based on an initial assessment formed through the analysis of hundreds of potential threat and/or attack scenarios, the Coast Guard will set annual and long-term targets for overall risk reduction, as well as for each of the three risk components – threat, vulnerability and consequence. These components map directly to the CMT strategic objectives of Prevent – Protect – Respond. Through an established process, principal program stakeholders will regularly assess the Coast Guard’s ability and success in reducing the level of risk,

by examining the Coast Guard's ability to bring its Authorities, Capabilities, Competencies and Partnerships (ACCP) to bear. These judgments will be directly informed by the suite of Tier II and III measures contained in Appendix C.

**Tier II Measures:** Tier II measures gauge CMT mission results at the intermediate outcome level and link the Coast Guard's activities to its wider strategic objectives and outcomes. These measures are designed to be examined and reported more frequently than the Tier I outcome measure, but will figure into the annual analysis of CMT mission outcome success. With appropriate accompanying context, these measures are suitable for periodic external reporting.

**Tier III Measures:** Tier III measures are designed for internal program management, and are focused more directly on the management of activity levels. These may be useful on a day-to-day basis, are examined more frequently than Tier I and II measures, but are not designed for external reporting.

The analysis of Tier I and II metrics will be most useful in adjusting and setting Activity Standards. Tier III metrics will be most useful in determining the degree to which Activity Standards are being achieved.

### **PERFORMANCE IMPROVEMENT**

We face an adaptive adversary, and security risks in our ports, waterways, coastal and offshore environments are dynamic. The adversary is working hard to obtain new destructive capabilities, but we will be working harder to stay ahead of this adversary. As we improve our prevention capabilities and reduce vulnerabilities, the adversary will adapt. The Coast Guard will aggressively employ threat-based risk management practices to ensure that we:

Maintain a current picture of terror-related risks in the maritime domain, accounting for all key independent variables, including evolving adversary capabilities and intentions,  
Develop new ways and means to deal with emerging risks,  
Evaluate and improve deployed ways and means, exploiting technological and tactical developments, and  
Adjust authorities, capabilities, competencies, and partnerships as required.

We will collaborate across the wide array of homeland security stakeholders in the spirit and letter of the Government Performance Review Act (GPRA) to maximize CMT performance value.

Most maritime terrorist scenarios are low-probability, high-consequence events. Our fundamental operational concepts and courses of action are well matched to the current and forecast environment. We will work hard to improve the understanding necessary to maximize risk-reduction return-on-investment.

## RESOURCING

Carefully crafted performance standards developed within a clear concept of operations shape functional requirements. Activity levels applied against risk drive total functional requirements—what kinds, in what quantities, where, and under what conditions. Three basic principles drive the development sequence:

- (1) Establish key initiatives and associated milestones to obtain and field effective, economical CMT implementing capabilities and capacity.
- (2) Lay critical systems foundations early.
- (3) Achieve the greatest possible risk reductions with minimal cost (optimal return on investment).

Determining appropriate resource requirements is dependent on clearly identifying:

- **Functional requirements** – Detailed, measurable requirements needed to perform the selected operational activities. Functional requirements are a direct result of analyzing problems/issues encountered during the execution of operational activities.
- **Implementing capabilities** – The people, training, equipment, supplies, information, and infrastructure necessary to satisfy operational requirements. Functional requirements may be satisfied by multiple implementing capabilities.

By studying the most likely, highest risk attack scenarios in the maritime domain, and then applying activities to mitigate those risks, the Coast Guard can produce a projection of the resources required to execute its strategy. Summation of the resource requirements across the spectrum of risk provides a service-wide projection of resource requirements to execute the CMT mission to achieve the stated objectives.

## KEY CMT INITIATIVES

This section identifies initiatives that will refine the ways, and build out the next increments of means – authorities, capabilities, competencies, partnerships, and capacity – to accomplish CMT objectives. These initiatives represent the best opportunities, over the next two to five years, to reduce maritime terror-related risk, based on our best understanding of threats, vulnerabilities, and consequences, within projected budget constraints.

### Overarching Initiatives

- National Security Presidential Directive 41/Homeland Security Presidential Directive 13 (NSPD-41 / HSPD-13)
- The National Strategy for Homeland Security and its eight supporting plans

### Awareness Initiatives

- Long range identification and tracking (LRIT/Sea View Vessel Tracking)
- Nationwide Automatic Identification System (NAIS)

- Notice of Arrival (NOA)
- National tracking of vessels carrying Certain Dangerous Cargo (CDC)
- Command Center 2010
- Common Operating Picture (COP)

#### Prevention / Protection Initiatives

- MTSA Compliance / Inspect vessel fleet
- Complete permits on time for offshore LNG Terminals
- National Maritime Transportation Security Plan
- Ferry VBIED procedures and technology development
- Maritime Security Risk Assessment Model (MS-RAM)
- Refine AMSPs and AMS Exercise program
- More accurate mariner credentialing
- Biometric identity validation
- Floating barriers
- Integrated Deepwater System (IDS)
- International Port Security Program
- Personal radiation detectors
- Explosive detection
- Maritime Safety and Security Teams (MSST) / Enhanced MSST (EMSST) (Maritime Security Response Team (MSRT))
- Airborne Use of Force (AUF)
- Underwater Port Security Measures
- Refine doctrine, TTP and training programs
- Identify and deploy better weapon systems
- Develop and institute readiness measurement program
- Continue expert analysis of maritime risk and effective mitigation strategies
- CBRNE search and detection capability

#### Response / Recovery Initiatives

- Sector Command Center Implementation
- National Response Options Matrix (NROM)
- Develop and institute response capability standards and readiness assessment program
- NRP / NIMS training
- Develop internal and external Continuity of Operations Plans (COOP)
- Maritime Safety and Security Teams (MSST) / Enhanced MSST (EMSST) (Maritime Security Response Team (MSRT))

## VI. SUMMARY - THE WAY AHEAD

As the Secretary of Homeland Security has noted, the task before us is a marathon not a sprint, and we are much nearer the start than the finish.

Drawing from the DHS strategic objectives of awareness, prevent, protect, respond and recover, *Maritime Sentinel* defines the Combating Maritime Terrorism mission. It sets forth plans to build toward terror-related risk-management readiness and performance maturity. *Maritime Sentinel* incorporates the key concepts of active deterrence, threat-based risk management, and layered defense.

The success of the CMT mission depends upon achieving Maritime Domain Awareness, effective maritime security and response operations, and the establishment of a maritime security regime. Within the construct of these three pillars, *Maritime Sentinel* identifies CMT activities and establishes standards for each.

Even as the ink dries on this document, we are busy refining our understanding of our enemies' capabilities and intent, our vulnerabilities and associated consequences. We are already embarked on the next mission development spiral with the objective of making best awareness, prevention, protection, response, and recovery progress against long-term risk-reduction return-on-investment value. The Coast Guard is collaboratively working in an interagency framework to optimally leverage the Service's unique authorities, and provide robust capacity and competency, including the conduct of offshore cordon and search procedures for vessels, as envisioned in the Maritime Operational Threat Response Plan. Progress towards the desired end state for the CMT mission will be captured in future versions of this document.

Additionally, we are coordinating with our national and international partners to improve our knowledge, to shape the environment, to lead active interventions, and to position the team for success in the daunting task of attaining Homeland Security in the maritime domain.

For the foreseeable future, we will revise this document as our understanding of this complex mission evolves.

## APPENDIX A: GLOSSARY AND ACRONYMS

### Glossary

**Antiterrorism (AT)**: Defensive measures used to reduce the vulnerability of individuals and property to terrorist acts. It includes physical and procedural security measures. (Source: DoD Dictionary of Military and Associated Terms, Joint Pub 1-02)

**Armed Aircraft**: An armed Coast Guard rotary wing aircraft crewed by personnel trained and qualified in airborne use of force, and equipped with one or more automatic fire and single shot or semi-automatic precision fire weapons. (Source OP Neptune Shield OPORD)

**Armed Vessel**: A government owned and operated vessel with a mounted, automatic firing weapon (e.g., .50 caliber machine gun, M-60, M-240, or MK 14 enhanced battle rifle) in addition to carrying the M-16 or shotgun, crewed by personnel trained and qualified in the Coast Guard's Use of Force Policy. (Source OP Neptune Shield OPORD)

**Boarding**: A boarding is an armed intervention led and conducted by uniformed and qualified Coast Guard personnel (accompanied by others as may be necessary and appropriate) aboard a vessel for the purpose of detecting and suppressing violations of applicable law. Activities undertaken by the Coast Guard that do not meet each of these requirements shall not be referred to as a "boarding." (Source: MLEM, COMDTINST M16247.1 (series)). See also "Security Boarding."

**Captain of the Port (COTP)**: The officer of the Coast Guard, under the command of a District Commander, so designated by the Commandant for the purposes of giving immediate direction to Coast Guard law enforcement activities within his assigned area. (Source: E 11249, 30 FR 13001, 33 CFR Ch 1, Sect 6.01-3; see also 14 USC 643)

**Combating Maritime Terrorism (CMT)**: The Coast Guard's CMT mission is to protect the U.S. Maritime Domain and U.S. Marine Transportation System (MTS); prevent terrorist attacks, sabotage, espionage, or subversive acts; and respond to and recover from those that do occur. CMT includes the employment of awareness activities; counterterrorism, antiterrorism, and response operations; and the establishment and oversight of a maritime security regime.

**Counterterrorism (CT)**: Operations that include offensive measures taken to prevent, deter, and respond to terrorism. (Source: DoD Dictionary of Military and Associated Terms, Joint Pub 1-02).

**Escort**: Provision of armed vessels and/or aircraft to enforce a moving security zone or naval vessel protection zone (NVPC), or otherwise accompany and protect against

external attack. The geographic extent of the escort shall be specified by the operational commander.

Federal Maritime Security Coordinator (FMSC): Coast Guard Captains of the Port (COTPs) are designated FMSCs. They are authorized to establish, convene, and direct the Area Maritime Security (AMS) Committee, appoint members to the AMS Committee, develop and maintain, in coordination with the AMS Committee, the AMS Plan, and implement and exercise the AMS Plan.

High Interest Vessel (HIV): A vessel intending to enter a U.S. port that may pose a high relative security risk.

High Value Unit (HVU): USN/NATO aircraft carriers; submarines; and Military Sealift Command (MSC) sealift / pre-positioned (PREPO) vessels carrying ammunition or other military essential cargo in support of actual combat operations (e.g., Operation Enduring Freedom and Operation Iraqi Freedom).

Inland waters: All U.S. Waters shoreward of the baseline from which the U.S. territorial sea is measured, including all waters on the U.S. side of the international boundary of the Great Lakes. (Source: 33 CFR 2.26)

Key Assets (KA): See MCI/KA.

Key port areas: Areas within ports or along navigable waterways where heavily populated areas, DoD assets, choke points, or MCI/KA would be vulnerable to attacks.

Marine Transportation System (MTS): The U.S. Marine Transportation System consists of waterways, ports and their intermodal connections, vessels, vehicles, and system users, as well as Federal maritime navigation systems. (Source: USCG Maritime Strategy for Homeland Security and the National Strategy for the MTS).

Maritime Critical Infrastructure/Key Assets (MCI/KA): Facilities, structures, systems, assets or services so vital to the port and its economy that their disruption, incapacity, or destruction would have a debilitating impact on defense, security, the environment, long-term economic prosperity, public health, or safety of the port. (Source: 33 CFR 101.105)

Maritime Domain: All areas and things of, on, under, relating to, adjacent to, or bordering on a sea, ocean, or other navigable waterway, including all maritime-related activities, infrastructure, people, cargo, and vessels and other conveyances. (Source: NSPD-41 / HSPD-13)

Maritime Domain Awareness (MDA): MDA is the effective understanding of anything associated with the maritime domain that could impact the security, safety, economy, or environment of the United States. (Source: National Plan to Achieve Maritime Domain Awareness)

Maritime Safety and Security Team (MSST): MSSTs are deployable teams designed to augment local USCG forces during periods of increased threat. Each MSST includes:

- Six 25-foot small boats,
- Eleven motor vehicles
- 75 Active Duty personnel

Several of the MSSTs also include:

- A dive team
- Canine explosive detection dog teams (K-9 EDD teams).

MSSTs can be deployed within 12 hours and are capable of establishing port security operations within four hours of arriving at their destination.

Military and Economically Strategic (MES) Ports: This term refers to the ports of greatest concern from a risk perspective. This term replaces the previously used term “Tiered Ports.” The MES ports account for approximately 95 percent of all maritime commerce.

Military Outload (MOL): Loading or unloading of military cargo or ammunition in support of actual or potential combat operations. (Source: Neptune Shield OPORD).

Naval Vessel Protection Zone (NVPZ): As described in 33 CFR 165, Subpart G, a NVPZ is a 500-yard regulated area of water, including a 100-yard exclusion zone, surrounding large U.S. Naval Vessels, including MSC vessels, in effect at all times in the navigable waters of the U.S. (out to 3nm), whether the large naval vessel is underway, anchored, moored, or within a floating drydock, except when the large naval vessel is moored within a restricted area or within a naval defensive sea area. (Source: 33CFR 165, Subpart G)

Patrol: Patrol is the action of traveling an area for observation or the maintenance of safety and security.

Positive Control Measures: Concurrent with or upon completion of a security boarding, armed boarding team members take up positions aboard the vessel to deter, detect, prevent, and respond to acts of terrorism and /or transportation security incidents. (Source: MLEM, COMDTINST M16247.1 (series))

Risk: The expected losses over time, based on the combined effects of threat, vulnerability, and consequence.

Security Boarding: An examination by an armed boarding team of a vessel (including the cargo, documentation, and persons on board), including vessels of interest (VOI), designated by the COTP or District / Area Commander, arriving or departing a U.S. port or offshore, to deter acts of terrorism and/or transportation security incidents. (Source: ALCOAST 506 / 05)

**Security Inspection:** A USCG inspection of a vessel or facility to verify compliance with the security regulations and its approved security plan.

**Terrorism:** Any activity that involves an act that (i) is dangerous to human life or potentially destructive of critical infrastructure or key resources; and (ii) is a violation of U.S. Criminal law or of any state or other subdivision of the U.S.; and appears to be intended (i) to intimidate or coerce a civilian population; (ii) to influence the policy of a government by intimidation or coercion; or (iii) to affect the conduct of a government by mass destruction, assassination, or kidnapping. (Source: the Homeland Security Act of 2002, section 2(15), codified at 6 USC 101(15))

**Transportation Security Incident:** A security incident resulting in a significant loss of life, environmental damage, transportation system disruption, or economic disruption in a particular area. (Source: 46 USC 70101)

**U.S. Maritime Domain:** The U.S. Maritime Domain encompasses all U.S. ports, inland waterways, harbors, navigable waters, Great Lakes, territorial seas, contiguous zone, customs waters, coastal seas, littoral areas, the U.S. Exclusive Economic Zone, and oceanic regions of U.S. national interest, as well as the sea lanes to the U.S., U.S. maritime approaches, and the high seas surrounding America. (Source: USCG Maritime Strategy for Homeland Security)

**Vessel of Interest (VOI):** A vessel identified by the National Maritime Intelligence Center (NMIC), area maritime intelligence fusion centers, district intelligence office, or other agency at the regional/port level as posing a potential security or criminal threat.

**Waterfront Facilities:** Piers, wharves, docks, or similar structures to which vessels may be secured and naval yards, stations, and installations, including ranges; areas of land, water, or land and water under and in immediate proximity to them; buildings on them or contiguous to them and equipment and materials on or in them. (Source: 33 CFR 6.01-4, as amended by Executive Order 13143 of December 1, 1999).

Note: This term is distinguished from the term facility, which means any structure or facility of any kind located in, on, under, or adjacent to any waters subject to the jurisdiction of the United States. This definition is applicable when enforcing chapter 701 of title 46 of the U.S. Code (Port Security) and implementing regulations promulgated pursuant to that chapter. The term facility is broader than the term waterfront facility because it is not limited to property in immediate proximity to mooring facilities and navy installations.

(Source: 46 USC 70101 (2))

**Weapon of Mass Destruction (WMD).** Any weapon that is intended to cause death or serious bodily injury through the release, dissemination, or impact of toxic or poisonous chemicals or their precursors; any weapon involving a disease organism; or any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. (Source: MLEM, COMDTINST M16247.1 (series))

## List of Acronyms

ACCP	Authorities, Capabilities, Competencies and Partnerships
AIS	Automatic Identification System
AMSC	Area Maritime Security Committee
AMSP	Area Maritime Security Plan
AT	Antiterrorism
AUF	Airborne Use of Force
C4ISR	Command, Control, Communications, Computers, Intelligence, Surveillance and Reconnaissance
CBRNE	Chemical, Biological, Radiological, Nuclear, or Explosive
CDC	Certain Dangerous Cargoes
CMT	Combating Maritime Terrorism
COTP	Captain of the Port
CT	Counterterrorism
DHS	Department of Homeland Security
DOD	Department of Defense
EDD Team	Explosive Detection Dog Team
EMSST / MSRT	Enhanced Maritime Safety and Security Team / Maritime Security Response Team
EOSO	Extended Offshore Security Operations
ESF	Emergency Support Function
FEMA	Federal Emergency Management Agency
FMSC	Federal Maritime Security Coordinator
FYHSP	Future Year Homeland Security Program
GAO	Government Accounting Office
GPRA	Government Performance Review Act
GT	Gross Tons
HCPV	High Capacity Passenger Vessel
HIV	High Interest Vessel
HSPD	Homeland Security Presidential Directive
HVA	High Value Asset
HVU	High Value Unit
IDS	Integrated Deepwater System
IMO	International Maritime Organization
IPSLO	International Port Security Liaison Officer
IPSP	International Port Security Program
ISPS	International Ship and Port Facility Security Code
K9	Canine
KA	Key Asset
LNG	Liquefied Natural Gas
LOOP	Louisiana Offshore Oil Port
LPOC	Last Port of Call
LRIT	Long-Range Identification and Tracking
MARSEC	Maritime Security
MCI	Maritime Critical Infrastructure

---

MDA	Maritime Domain Awareness
MES	Militarily and Economically Strategic Ports
MHD	Maritime Homeland Defense
MHS	Maritime Homeland Security
MIFC	Maritime Intelligence Fusion Center
MOL	Military Outload
MOTR	Maritime Operational Threat Response
MSC	Military Sealift Command
MSST	Maritime Safety and Security Team
MTS	Marine Transportation System
MTSA	Maritime Transportation Security Act of 2002
NAIS	Nationwide Automatic Identification System
NATO	North American Treaty Organization
NCTC	National Counterterrorism Center
NMIC	National Maritime Intelligence Center
NMTSP	National Maritime Transportation Security Plan
NOA	Notice of Arrival
NPOC	Next Port of Call
NROM	National Response Options Matrix
NRP	National Response Plan
NSPD	National Security Presidential Directive
NSSE	National Special Security Event
NVPZ	Naval Vessel Protection Zone
OCS	Outer Continental Shelf
ONS	Operation Neptune Shield
PCM	Positive Control Measure
PDD	Presidential Decision Directive
PREPO	Pre-Positioned
PSI	Proliferation Security Initiative
PWCS	Ports, Waterways and Coastal Security
RBDM	Risk-Based Decision-Making
RB-M	Response Boat - Medium
ROI	Return on Investment
SAR	Search and Rescue
SCC	Sector Command Center
SIV	Special Interest Vessel
SPOD	Seaport of Debarkation
SPOE	Seaport of Embarkation
TSI	Transportation Security Incident
TTP	Tactics, Techniques and Procedures
U.S.C.	U.S. Code
VBIED	Vessel-Borne (or Vehicle-Borne) Improvised Explosive Device
VOI	Vessel of Interest
VTS	Vessel Traffic Service
WMD	Weapons of Mass Destruction



**Homeland Security**

**APPENDIX B: CMT ALIGNMENT TO DHS STRATEGIC PLAN (2004)**

Strategic Goals / 2SR Imperatives	Objectives <span style="float: right;">(USCG CMT mission alignment to DHS Strategic Plan)</span>
<p><b>Awareness</b> - Identify and understand threats, assess vulnerabilities, determine potential impacts, and disseminate timely information to our homeland security partners and the American public.</p> <p><b>2SR Imperative:</b> Information Sharing</p>	<p><b>1.1 Gather and fuse all terrorism related intelligence; analyze and coordinate access to information related to potential terrorist or other threats</b></p> <p>1.2 Identify and assess the vulnerability of critical infrastructure and key assets</p> <p>1.3 Develop timely, actionable and valuable information based on intelligence analysis and vulnerability assessments</p> <p><b>1.4 Develop a Common Operating Picture for Domestic situational awareness, including land, sea, and air.</b></p>
<p><b>Prevention</b> - Detect, deter, and mitigate threats to our homeland</p> <p><b>2SR Imperative:</b> Borders &amp; Immigration Transportation Security</p>	<p><b>2.1 Secure our borders against terrorists, means of terrorism, illegal drugs and other illegal activity</b></p> <p>2.2 Enforce trade and immigration laws</p> <p>2.3 Provide operational end users with the technology and capabilities to detect and prevent terrorist attacks, means of terrorism and other illegal activities</p> <p>2.4 Ensure national and international policy, law enforcement and other actions to prepare for and prevent terrorism are coordinated 11, RB-M, IDS</p> <p><b>2.5 Strengthen the security of the Nation's transportation systems</b></p> <p>2.6 Ensure the security and integrity of the immigration system</p>
<p><b>Protection</b> - Safeguard our people and their freedoms, critical infrastructure, property, the economy of our nation from acts of terrorism, natural disasters, or other emergencies</p> <p><b>2SR Imperative:</b> Transportation Security Preparedness</p>	<p><b>3.1 Protect the public from acts of terrorism and other illegal activities</b></p> <p>3.2 Reduce infrastructure vulnerability from acts of terrorism</p> <p>3.3 Protect against financial and electronic crimes, counterfeit currency, illegal bulk currency movement and identity theft</p> <p>3.4 Secure the physical safety of the President, Vice President, visiting world leaders and other protectees</p> <p>3.5 Ensure the continuity of government operations and essential functions in the event of crisis or disaster</p> <p>3.6 Protect the marine environment and living marine resources</p> <p>3.7 Strengthen nationwide preparedness and mitigation against acts of terrorism, natural disasters, or other emergencies</p>
<p><b>Response</b> - Lead, manage, and coordinate the national response to acts of terrorism, natural disasters, or other emergencies</p> <p><b>2SR Imperative:</b> Preparedness</p>	<p><b>4.1 Reduce the loss of life and property by strengthening nationwide response readiness</b></p> <p><b>4.2 Provide scaleable and robust all-hazard response capability</b></p> <p>4.3 Provide search and rescue services to people and property in distress</p>
<p><b>Recovery</b> - Lead national, state, local, and private sector efforts to restore services and rebuild communities after acts of terrorism, natural disasters, or other emergencies</p>	<p>5.1 Strengthen nationwide recovery plans and capabilities</p> <p>5.2 Provide scaleable and robust all-hazard recovery assistance</p>
<p><b>Service</b> - Serve the public effectively by facilitating lawful trade, travel and immigration</p>	<p>6.1 Increase understanding of naturalization, and its privileges and responsibilities</p> <p>6.2 Provide efficient and responsive immigration services that respect the dignity and value of individuals</p> <p>6.3 Support the United States humanitarian commitment with flexible and sound immigration and refugee programs</p> <p>6.4 Facilitate the efficient movement of legitimate cargo and people</p>
<p><b>Organizational Excellence</b> - Value our most important resource, our people. Create a culture that promotes a common identity, innovation, mutual respect, accountability, and teamwork to achieve efficiencies, effectiveness, and operational synergies</p>	<p>7.1 Protect confidentiality and data integrity to ensure privacy and security</p> <p>7.2 Integrate legacy services within the Department improving efficiency and effectiveness</p> <p>7.3 Ensure effective recruitment, development, compensation, succession management and leadership of a diverse workforce to provide optimal service at a responsible cost</p> <p>7.4 Improve the efficiency and effectiveness of the Department, ensuring taxpayers get value for their tax dollars</p> <p>7.5 Lead and promote E-government modernization and interoperability initiatives</p> <p>7.6 Fully integrate the strategic planning, budgeting and evaluation processes to maximize performance</p> <p>7.7 Provide excellent customer service to support the mission of the Department</p>

## **APPENDIX C: ACTIVITIES, STANDARDS, AND METRICS**

Standards are classified and published separately.