Maritime Modal Implementation Plan

Table of Contents
Maritime Modal Annex

1 Executive Summary

Salt water covers more than two-thirds of the earth's surface. These waters comprise an immense maritime domain,[1] a continuous body of water that is the earth's greatest defining geographic feature. Ships that ply the maritime domain are the primary mode of transportation for world trade, carrying more than 80 percent[2] of the world's trade by volume. United States maritime trade is integral to the global economy, representing more than 20 percent[3] of global maritime trade. Through the Maritime Transportation System (MTS),[4] the maritime mode is the primary transportation mode providing connectivity between the U.S. and global economies; 99 percent of overseas trade by volume enters or leaves the U.S. by ship.[5] The MTS enables the U.S. to project military presence across the globe, creates jobs that support local economies, and provides a source of recreation for all Americans. The Nation's economic and military security are fundamentally linked to the health and functionality of the MTS.[6]

The security of the MTS is paramount to protecting the Nation and its economy, but it presents daunting and unique challenges to managers of the Maritime Mode. Security of the MTS is intrinsically linked to the security of the maritime domain which contains critical infrastructure and key resources (CI/KR) from many of the other critical infrastructure sectors and Transportation Sector modes. Providing for the security of the MTS depends upon understanding the diverse array of activities in the maritime domain through the transparency of all sector and transportation modal infrastructure and security activities.

The October 2005 National Maritime Transportation System Security Recommendations for the National Strategy for Maritime Security describe the Maritime Transportation System Security as:

> A systems-oriented security regime built upon layers of protection and defense in-depth that effectively mitigates critical system security risks, while preserving the functionality and efficiency of the MTS. Understanding the most effective security risk management strategies involves cooperation and participation of both domestic and international stakeholders acting at strategic points in the system, the U.S. seeks to improve security through a cooperative and cohesive effort involving all stakeholders.

The maritime transportation Security Partners will achieve a safer, more secure, efficient, and resilient MTS through the cooperative pursuit of actions that mitigate the overall risk to the physical, cyber, and human CI/KR assets and resources of the system and its interconnecting links with other modes of transportation and CI/KR sectors.

---

[1] The National Strategy for Maritime Security (NSMS) defines the maritime domain as 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. Note: The maritime domain for the United States includes the Great Lakes and all navigable inland waterways such as the Mississippi River and the Intra-Coastal Waterway.

[2] Organization for Economic Co-operation and Development, *Security in Maritime Transport: Risk Factors and Economic Impact,* Maritime Transport Committee, July 2003, p. 6.

[3] National Chamber Foundation of the U.S. Chamber of Commerce, *Trade and Transportation, A Study of North American Port and Intermodal Systems,* Washington, D.C., March 2003, p. 1.

[4] Also referred to as the Marine Transportation System. In context of the Transportation Systems Sector, the U.S. Coast Guard is the Sector Specific Agency for the maritime transportation mode, which may be also referred to as the maritime transportation systems mode.

[5] Committee on the Maritime Transportation System, *What is the MTS?,* http://www.cmts.gov//whatismts.htm, last accessed 2 Nov 2006.

[6] Interagency task Force on Coast Guard Roles and Missions, *A Coast Guard for the Twenty-First Century: Report of the Interagency task Force on U.S. Coast Guard Roles and Missions,* December 1999.

- Maritime modal stakeholders are formalizing new coordination processes using the Sector Partnership Model espoused in the National Infrastructure Protection Plan (NIPP). The Maritime Modal Government Coordinating Council (MMGCC) has formed and the Maritime Modal Sector Coordinating Council (MMSCC) is in development.
- The promotion of Maritime Domain Awareness (MDA), which allows for the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the U.S. MDA is a foundational element of maritime security and CI/KR protection. It will enhance information-sharing among Federal, State, local, and tribal authorities; the private sector; and international partners. This enriched information will be used by decision makers in determining response and risk management calculations for protecting Maritime CI/KR and in turn the overall MTS.
- The Maritime Security Risk Assessment Model (MSRAM) assesses and manages risk for maritime infrastructure. A systems approach to risk management is being developed to improve efficiencies of resources and increase modal security.

2 Overview of Mode

The maritime transportation mode is unique in both its management and composition. The unique qualities of the mode present extraordinary complexity and challenges to those charged with the security of maritime CI/KR and systems.

No single government agency possesses the responsibility for, the resources required, or the awareness needed, to ensure the security in the maritime mode. The security of the mode depends on the cooperative actions of multiple Federal, State, local, tribal, and private entities, in addition to international partners. Prior to the NIPP, many varied processes provided the means for interagency coordination, including Policy Coordinating Committees, work groups, liaison officers, and Memorandums of Understanding (MOUs). While these means for coordination will continue, new constructs are being formed in accordance with the NIPP Partnership Model in an effort to better enable coordinated security across transportation modes.

The U.S. Coast Guard (USCG), as the Sector Specific Agency (SSA) for the maritime transportation mode will continue to work collaboratively with the Transportation Security Administration (TSA), Customs and Border Protection (CBP), and other Federal agencies, State, local, and tribal entities as the chair of the MMGCC. The MMGCC will work with industry security partners[7] to implement NIPP requirements of CI/KR protection, and to help prevent, prepare for, protect against, respond to, and recover from transportation security incidents (TSI), natural disasters, and other emergencies.[8] Other security partnerships include international cooperation vis-à-vis participation in international organizations, other multilateral and bilateral forums, and exchanges.

The MTS is a complex system that is geographically and physically diverse in character and operation. From a systems perspective, the MTS is a network of maritime operations that interface with shore-side operations at intermodal connections as part of the overall global supply chains or domestic commercial operations. The various maritime operations within the MTS networks have components that include vessels, port facilities, waterways and waterway infrastructure, and intermodal connections and users, including crew, passengers, and workers.

MTS components share critical interfaces with each other with limited and selective overarching information systems. Improving security of the MTS focuses on four primary elements: 1) Component Security, 2) Interface Security, 3) Information Security, and 4) Network Security. MTS component security ensures that individual physical components have measures in place to prevent exploitation, protect against terrorist attack, contain incidents that do occur, and recover from incident effects. MTS interface security provides for coordinated security measures between modes of transportation and at key interactions between MTS components and functions. MTS information security ensures that key data systems are not corrupted or exploited and are available to support maritime operations while also providing protected availability of proprietary information needed to support security planning and implementation. Network security is the big picture view that focuses on enhancing security through overarching systems that facilitate performance of the MTS and provide effective coordination among stakeholders at the policy and senior management levels.

[7] See Glossary of Key Terms NIPP, June 2006.

[8] The NIPP and the National Response Plan (NRP) together provide a comprehensive, integrated approach to the homeland security mission.

The maritime domain also contains CI/KR from many of the other critical infrastructure sectors and transportation sector modes. Providing for the security of the maritime mode depends upon understanding all activities in the maritime domain through the transparency of all sector and transportation modal infrastructure and security activities. The MTS and component CI/KR function as intermodal gateways for cargo flow to and from other CI/KR sectors. Significant economic and functional dependence exists within the transportation system on the timely and free flow of maritime commerce to and from homeland destinations. Because of the complexity, these interdependencies require any maritime security planning to be coordinated and aligned with any connecting transportation mode or sector.

The largest aggregation of cargo within the Transportation Systems Sector occurs in ports—in vessels, cargo transfer and storage nodes, and intermodal connections. All are, to varying degrees, potential targets. The effects of cargo and conveyance, combined with close proximity with surrounding industrial areas and communities, magnify the potential consequences of even a single-facility or single-vessel TSI with potential effects well outside of the maritime domain. Vessels, containers, cargo, and commercial vehicles are also potential media for smuggling and infiltration of weapons and perpetrators, as well as potential conveyances of devices for direct attacks on port complexes.

The National Strategy for Maritime Security (NSMS) defines MDA as "the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy or environment of the United States." The product of MDA is knowledge used by decision makers to determine appropriate responses to maritime threats or to conduct further analysis. MDA is broken down into four activities; collection, fusion, analysis and dissemination. Data and information on people, cargo, vessels, and infrastructure associated with the maritime domain are collected. (Collection is from all sources: classified sources, regulatory data, industry data, law enforcement, military, open source, etc.) The data are then fused and analyzed to provide situational awareness and reveal anomalies and patterns. The resultant intelligence and information are then available via a variety of communication channels. MDA includes concerted efforts of Federal, State, local, and tribal authorities in conjunction with commercial stakeholders, foreign governments, and other international partners. MDA is a foundational element for security and CI/KR protection as the associated activities and results encompass the maritime domain and MTS. The knowledge provided through the MDA effort can be used by decision makers in their response decisions and risk management calculations.

Maritime security partners will continue to work cooperatively to improve the existing baseline of maritime security planning efforts. Improvements to maritime homeland security will continue to build on lessons learned from ongoing operations, incident management training and exercises, research and development, science and technology, improved common operating picture through improved MDA and enhanced, interoperable information-sharing mechanisms.

3 The Maritime Transportation Mode

As previously discussed, the MTS is a highly complex system that is both geographically and physically diverse in character and operation**.** The MTS consists of waterways, ports and intermodal landside connections, which allow the various modes of transportation to move people and goods to, from and on the water. The MTS includes the following:[9]

- 25,000 miles of navigable waters
- 238 locks at 192 locations
- The Great Lakes
- Saint Lawrence Seaway
- More than 3,700 marine terminals
- More than 1,400 intermodal connections

The maritime domain of the U.S. consists of more than 95,000 miles of coastline, 360 ports, 3.4 million square miles of Exclusive Economic Zones, and thousands of bridges, dams, and levees. The task of protecting the MTS is enormous and essential to maintaining the security of the U.S. economy as shown by the following representative facts:[10]

- Waterborne cargo and associated activities contribute more than $742 billion annually to the U.S. gross domestic product (GDP), sustaining more than 13 million jobs
- In 2004, approximately 6,400 commercial ships made approximately 60,000 U.S. port calls carrying more than 6 million cargo containers to the U.S.
- In 2003 alone, more than 1.2 billion short tons of international maritime cargo were transported through U.S. seaports.
- Ninety-nine percent of the volume of overseas trade (62 percent by value) enters or leaves the U.S. by ship.

3.1 Vision and Goals[11]

The vision and goals of the Maritime Transportation Mode are:

Vision. Through partnering, sustain a secure and efficient MTS that enables legitimate travelers and goods to move without fear of harm, reduction of civil liberties or disruption of commerce.

Goal 1: Prevent and deter acts of terrorism against the, or involving use of, MTS.
Objectives: (a) Security partners will continue to develop and implement flexible, layered, security measures, both routine and random, while increasing security awareness training and security information-sharing. (b) Security partners will conduct combined drills and exercises to test, practice, and evaluate the execution of prevention/protection operations and contingency plans and procedures.

Goal 2: Enhance resiliency of the MTS
Objective: (a) Security partners will reduce the risk associated with key nodes, links and flows within critical MTSs to enhance overall MTS survivability and continue to develop flexible contingency plans that are exercised and updated to ensure the most expeditious response and recovery to all-hazards events.

Goal 3: Maximize cost effectiveness for limited resources of the MTS[12]*.*
Objectives: (a) Security partners will strive to align resources to the highest priority of MTS

[9] Additional information available at Committee on the Marine Transportation System, *What is the MTS?, http://www.cmts.gov//whatismts.htm.*
[10] *Id*
[11] See TSSP Base Plan for Transportation Systems Sector Goals.

security risks and continue to develop and disseminate standards for risk analysis tools and methodologies. (b) Define physical, cyber, and human elements in relation to the protection of maritime CI/KR.

3.2 Unique Characteristics of the Maritime Mode

The MTS depends on networks of critical infrastructure—both physical networks such as the marine transportation system, and cyber networks such as interlinked computer operations systems. The ports, waterways, and shores of the maritime transportation mode are lined with military facilities, nuclear power plants, locks, oil refineries, levees, passenger terminals, fuel tanks, pipelines, chemical plants, tunnels, cargo terminals, and bridges.

Ports, in particular, have inherent security vulnerabilities: they are sprawling, easily accessible by water and land, close to crowded metropolitan areas, and interwoven with complex transportation networks. Port facilities, along with the ships and barges that transit port waterways, are especially vulnerable to tampering, theft, and unauthorized persons gaining entry to collect information and commit unlawful or hostile acts.

The CI/KR within the maritime sector constitutes a vital part of the complex systems necessary for public well-being, as well as economic and national security. They are essential for the free movement of passengers and goods throughout the world. Some physical and cyber assets, as well as associated infrastructure, also function as defense critical infrastructure; their availability must be constantly assured for national security operations worldwide. Just-in-time methods, utilized within industries, must be considered for their implications on risk and vulnerability. Beyond the immediate casualties, the consequences of an incident on one node of maritime critical infrastructure may include disruption of entire systems, cause congestion and limit capacity for product delivery, cause significant damage to the economy, or create an inability to project military force. Protecting maritime infrastructure networks must address individual elements, as well as intermodal aspects and their interdependencies positioned both within a regulatory environment, and a system of systems.

3.2.1 Key Components

Seaports and Marine Terminals
There are about 70 deep-draft port areas along U.S. coasts, including approximately 40 that each handle 10 million or more tons of cargo per year. Within these ports are approximately 2,000 major terminals. Most of these terminals are owned by port authorities and are operated by the private sector. Marine terminals and their associated berths are often specialized to serve specific types of cargo and passenger movements. Terminals handling bulk cargoes such as petroleum, coal, ore, and grain are frequently sited outside the boundaries of organized public port authorities. These facilities are often the origin and destination points for bulk commodities, and thus they differ from terminals often found in public ports, where shipments are transferred from one mode to another. Terminals handling containerized cargo tend to be located within larger public port complexes with significant warehousing, storage, and intermodal transportation connectivity. Container terminals at 15 ports account for 85 percent of all containership calls in the U.S., and the port complexes in six areas account for approximately 65 percent of these calls. These six areas are Long Beach–Los Angeles, New York–Newark–Elizabeth, San Francisco–Oakland, Hampton Roads, Charleston, and Seattle–Tacoma. Tanker calls are likewise concentrated regionally. They are most frequent in areas with significant petrochemical industries, such as the Gulf Coast, Delaware Bay, New York Harbor, San

[12] To the greatest extend possible under law.

Francisco Bay, and San Pedro Harbor. The ports in southern Louisiana are the centers of dry bulk grain traffic, most of which moves down the Mississippi River for export on larger oceangoing ships.

Terminal Facilities
Hundreds of natural and manmade harbors are situated along the U.S. coastline, and several contain federally maintained channels used regularly by both passenger and cargo vessels. Located on the waterfront are publicly and privately owned marine terminals that consist of piers and berths for vessel docking. Most are privately operated and are designed to handle particular types of commodities. The terminal may be a stand-alone facility on the shoreline or part of a system of terminals and other marine service facilities (e.g., tugboat operators, fuel depots, ship repair facilities) that together make up a larger port complex. Individual terminals are usually connected to rail sidings, roads that accommodate trucks, and pipelines. The terminal itself may be the origin or destination point for the cargoes moved on the waterways, as is the case for coal shipped to the dock of a waterfront power plant or chemicals shipped from a waterfront chemical plant.

Navigation Infrastructure and Services
U.S. waterways consist of thousands of miles of main channels, connecting channels, and berths. More than 90 percent of U.S. maritime trade passes through the more than 300 deep-draft navigation projects the U.S. Army Corp of Engineers (USACE) maintains nationwide. USACE's responsibilities for inland waterways are complemented by the Department of Commerce National Oceanic and Atmospheric Administration's (NOAA) responsibilities for coastal management; to chart, preserve, enhance, and monitor the condition of the nation's coastal resources and ecosystems. NOAA also manages the land, aerial and orbital infrastructure supporting NOAA's development and issuance of marine weather forecasts, watches and warnings. The USCG maintains nearly 50,000 aids to navigation that range from lighted buoys and beacons to radio navigation systems. Responsibility for waterway management, including coordinating and controlling vessel operations and scheduling on the waterways also includes, in addition to Federal agencies, local pilot associations, private marine exchanges, Port Authorities, and individual vessel operators.

Intermodal Connections
Intermodal transportation refers to a system that connects the separate transportation modes, such as aviation, maritime, mass transit, highways, and railroads, and allows a passenger or cargo to complete a journey using more than one mode. In terms of cargo transportation, an intermodal shipment is generally considered to be one that moves by two or more modes during a single trip. Intermodal connections link the various transportation modes—maritime ports and related facilities, highways, rail, and air.

Oceangoing Vessels
Major classes of oceangoing vessels are tankers, containerships, dry bulk and general cargo freighters, and specialized ships such as the roll-on/roll-off carriers used to transport motor vehicles. U.S. ocean ports and terminals handle more than 75,000 vessel calls per year. About two-thirds of these calls are made by tankers, containerships, and dry bulk carriers.

Passenger Carriers
Many of the passenger vessels operating in U.S. territorial waters are ferries. Many carry automobiles and trucks as well as passengers. Although they are important parts of the public transportation systems in cities such as Seattle, San Francisco, and New York, passenger ferries account for a small percentage of the Nation's total passenger trips on all public

transportation modes, including subways and urban buses. Likewise, passenger ocean liners no longer have significant roles in long-distance passenger transportation: they have been replaced by jet-liners. Cruise ships continue to serve the recreation and tourism industries and operate on a regular basis from U.S. ports. In 2005, more than nine million North Americans went on a cruise. The cruise industry also supports the economy. In 2004, cruise lines and their passengers spent $14.7 billion on U.S. goods and services and supported over 315,000 American jobs.[13]

Inland River, Coastal, and Great Lakes Systems

While the deep oceans are the primary means of moving cargo internationally, the U.S. inland river, coastal, and Great Lakes waterways are important means of moving ocean-borne cargo internally and for providing outbound feeder traffic for overseas shipping.

- *Inland River Systems*
  By far the largest and busiest inland waterway system in the U.S. is the Mississippi River system, which includes the large Ohio River and Missouri River tributaries. This system extends for more than 12,000 miles and encompasses navigable waterways on more than a dozen tributary systems passing through 17 states leading to the Gulf of Mexico. Barges are loaded and unloaded at shallow-draft terminals situated along the riverbanks. There are more than 1,800 shallow-draft terminal facilities in the U.S.

- *Coastal and Intracoastal Waterways*
  The main coastwise shipping activity in the U.S. occurs along the Gulf Coast and, to a lesser extent, along the Atlantic Coast. The Gulf Intracoastal Waterway (GIWW) is maintained by the USACE for 1,300 miles from Texas to Florida, is used for moving grain, coal, refinery products, and chemicals domestically and for supplying feeder traffic to seaports.

- *Great Lakes System*
  About 350 terminals are situated along the U.S. shoreline of the Great Lakes. A half-dozen lake ports rank among the top 50 U.S. ports in terms of tonnage, including Duluth–Superior, Chicago, Detroit, and Cleveland. The terminals in these ports, as well as most others on the Great Lakes, primarily handle dry bulk cargoes, led by iron ore, grain, coal, sand, stone, and lumber. Icebreaking operations maintain maritime travel and trade routes, allowing for mobility of law enforcement, defense assets, and essential resources. Access to, and transit within, the Great Lakes system requires close international cooperation with Canada.

Defense Port and Facility Prioritization

The DOD may require priority use of commercial port and intermodal facilities and services to meet military deployment or other defense emergency requirements. Pursuant to the Defense Production Act of 1950 (DPA), the Maritime Administration (MARAD) has authority (Title 46 Code of Federal Regulations [CFR], Part 340), delegated from the Secretary of Transportation, to require priority use of commercial port facilities and services by DOD ahead of commercial port contractual obligations. MARAD also has in place standby Federal Port Controller (FPC) service agreements (Title 46 CFR, Part 346) with key executives at fifteen U.S. ports. Each FPC is responsible for prioritizing and controlling the utilization of port facilities, equipment, and services to ensure military deployment cargo movement timelines are met, while minimizing congestion and disruption to the movement of commercial cargo. The National Port Readiness

[13] International Council of Cruise Lines, *Inside Cruising: A Guide for Travel Professionals,available at* http://www.iccl.org/faq/cruising.cfm, accessed on 24 November 2006.

Network (NPRN) helps train port and DOD personnel in using relevant emergency procedures and coordinates deployments through ports. The NPRN comprises nine Federal agencies, [MARAD, U.S. Transportation Command (USTRANSCOM), USCG, TSA, U.S. Northern Command [NORTHCOM], SDDC, USACE, MSC, and U.S. Forces Command (USFORSCOM)] with missions that support the secure movement of military cargo during deployments or other national emergencies. This training and coordination is accomplished through the local NPRN Port Readiness Committees.

3.2.2 Regulatory Environment

Security Partners derive their responsibilities, both individually and collectively, from several main sources: international agreements, treaties and conventions, legislation, executive directives, and assigned mission(s). Security Partners have worked collectively and collaboratively to meet these responsibilities and to create a layered security regime. This layered regime includes the International Maritime Organization's International Ship and Port Facility Security Code (ISPS Code), which was championed by the U.S. and other contracting governments, and has since been implemented and continues to be monitored by the U.S. and other member states around the globe. The Maritime Transportation Security Act of 2002 (MTSA, Public Law 107-295), developed contemporaneously with the ISPS Code, implements security requirements on the U.S. maritime industry.

Figure 3-1 depicts some of the multiple executive and legislative requirements for maritime security planning that required the collaborative efforts of all maritime stakeholders. It also depicts the relationships between these planning efforts.

Security partners recognize that while not all these responsibilities and requirements are derived for the explicit purpose to protect critical infrastructure, most support infrastructure protection and indirectly support the NIPP.

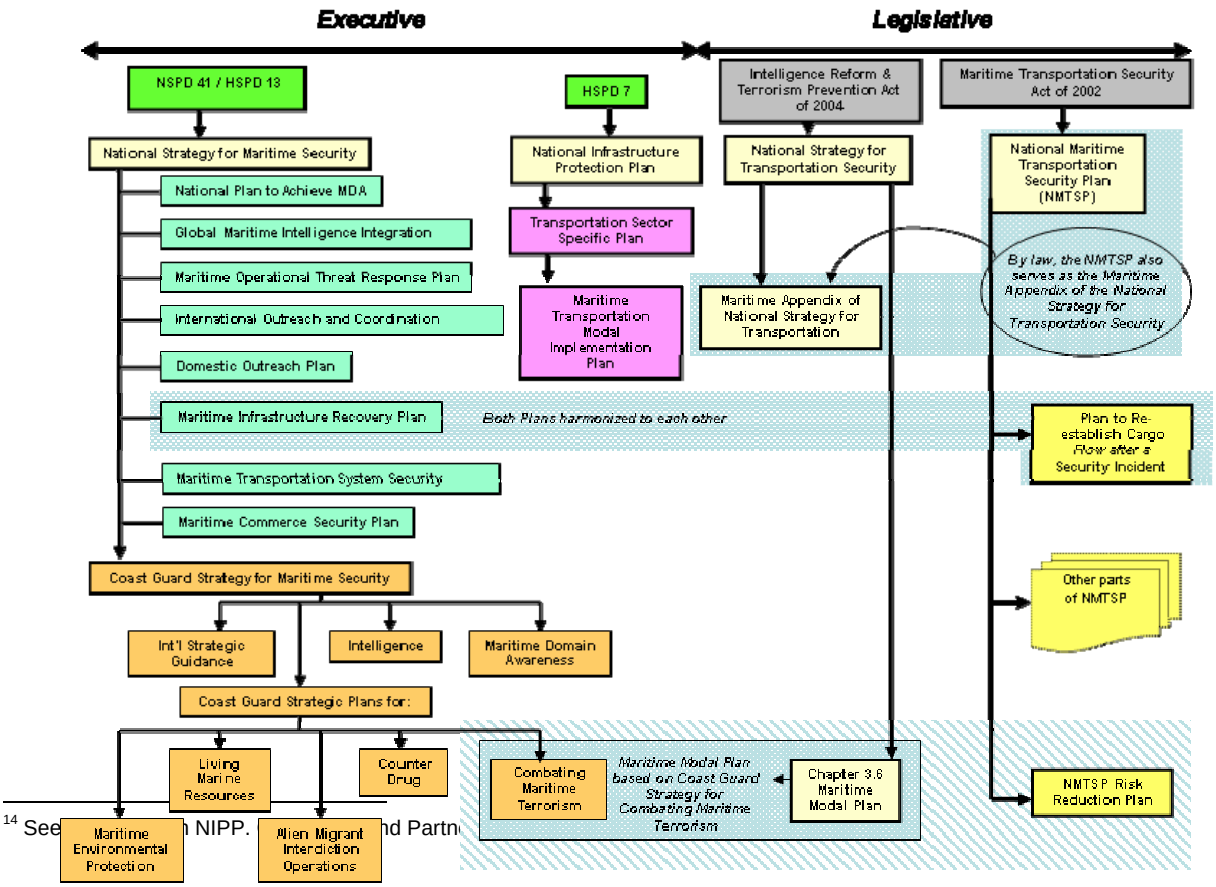
3.3 NIPP Partnership and Information-Sharing Processes

As described in the NIPP and the Transportation Sector-Specific Plan (TSSP) Base Plan, a network approach is used for information-sharing among security partners in order to share and protect the information needed to analyze risk and make risk-based decisions to protect CI/KR. The NIPP defines the organizational structure that provides the framework for coordinating CI/KR protection efforts at all levels of government, as well as within and across sectors. Sector-specific planning and coordination are addressed through private sector and Government Coordinating Councils (GCCs) that are established for each sector. Sector Coordinating Councils (SCCs) are comprised of private sector representatives of the SSAs; other Federal departments and agencies; and State, local, and tribal governments. These councils create a structure through which representatives from all levels of government and the private sector can collaborate or share existing consensus approaches to CI/KR.[14]

3.3.1 Existing Process of Information-Sharing

Information-sharing between security partners is vital to the protection of CI/KR and the application of the NIPP risk management framework—from setting security goals to identifying assets, systems, and network functions; to assessing the consequences, vulnerabilities and

Figure 3-1: Example Maritime Security Planning Requirements



[14] See NIPP. nd Partn

threats; to prioritizing and implementing protective programs and their measures of effectiveness. Multiple information-sharing processes are in use by the government and the private sector. Information is often shared through public meetings such as Shipping Coordinating Committee Meetings or other Federal Register Notifications. Effective practices include information-sharing vis-à-vis the Information-Sharing and Analysis Center (ISAC), HOMEPORT, Area Maritime Security Committees (AMSCs), and through more recent initiatives such as the NIPP Partnership Model. The following information-sharing mechanisms are specific to the maritime transportation mode.

ISAC[15]

The Maritime ISAC is unique from other CI/KR ISACs in that it is not managed by the private sector. It is currently managed by the USCG Office of Port Activities and serves the purpose of facilitating the sharing of security, critical infrastructure, and threat information with government and industry maritime security and critical infrastructure partners. Currently, the primary function of the Maritime ISAC is to serve as the focal point for gathering and disseminating information regarding maritime threats to interested stakeholders.

The ISAC operates at the national, regional and local levels and 1) provides information on threats to the MTS as well as information concerning incidents, threats, attacks, and vulnerabilities; 2) processes and analyzes incoming information in terms of which maritime stakeholder groups need the information and disseminates threat warning products to maritime stakeholders in a timely manner; 3) enables the maritime community to identify, report, and share information to reduce security vulnerabilities; and 4) facilitates the discussion and development of best practices and solutions on subsector and cross-sector issues between private and public sector stakeholders. The Maritime ISAC draws from multiple information sources from the national to local levels of the public and private sectors. Currently, the ISAC leverages the technology of HOMEPORT, as an organized mechanism for the secure exchange, dissemination, coordination, and storage of sensitive information.

Providing a two-way information-sharing process between maritime industry stakeholders and the government is under consideration for future development within the construct of the Maritime ISAC. Overall, the ISAC assists the maritime industry and State and local agencies with strengthening the Nation's capabilities to prevent, detect, respond to, and recover from potential TSIs on the MTS.

HOMEPORT[16]

HOMEPORT is a publicly accessed and a secure enterprise Internet portal that supports port security functionality for operational use. It also serves as the USCG's primary communication tool to support the sharing, collection, and dissemination of Sensitive but Unclassified (SBU) information, including Sensitive Security Information (SSI), For Official Use Only (FOUO), and Law Enforcement Sensitive (LES).

HOMEPORT meets the critical mission requirements in support of MTSA for information-sharing and is used as a primary means for day-to-day management and communication of port security matters between public and private security partnerships from the national to the local levels including coordination and collaboration between Federal Maritime Security Coordinators (FMSC) and AMSC members, commercial vessel and facility owners and operators, government partners, and the public.

[15] In 2003, under industry advisement, a maritime ISAC was formed; it is facilitated by Office of Port and Facility Activities at U.S. Coast Guard Headquarters in Washington, D.C.

[16] Additional information on Homeport available at http://homeport.uscg.mil

Area Maritime Security Committees

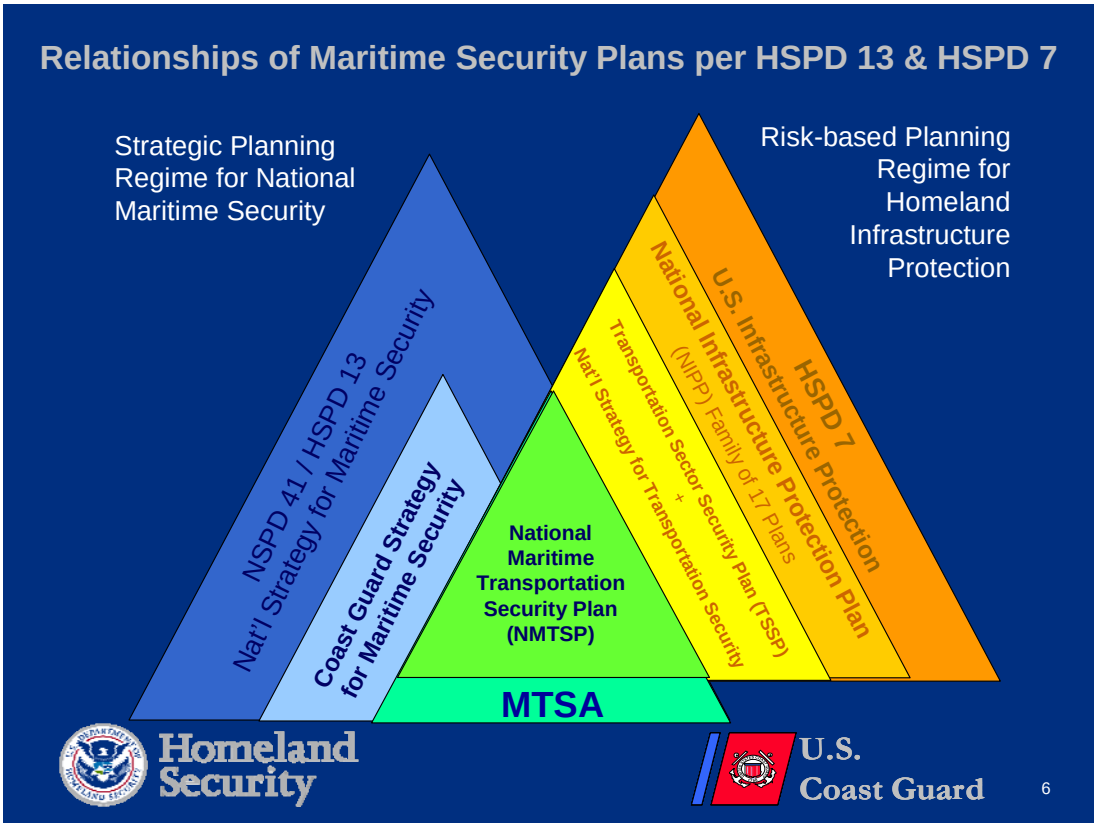
The USCG sponsors AMSCs to support all Captain of the Port zones. The AMSCs fall under the cognizance of a USCG FMSC, who is also the USCG Captain of the Port for a particular port area or zone. AMSCs are a cornerstone of U.S. national maritime security by serving as formal bodies at the local (and sometimes regional) level for coordinating and collaborating among various Federal, State, and local authorities and private sector maritime stakeholders for enhancing and maintaining port security within a given area.

4 Implementation Plan

As discussed in other sections of this document, the security of the maritime domain and its inclusive infrastructure is not the province of any single security partner; it is the collective, collaborative effort of Federal, State, local, tribal, and private sector security partners. While security partners share and support the goals in section 3.1, each pursues these goals in accordance with its own requirements (i.e., business, mission, executive, or legislative). Government security partners execute their responsibilities either individually or as part of a larger collaborative effort by enforcing Federal regulations, programs, plans, and strategies. These cumulative activities implement the responsibilities of the security partners which include, but are not limited to, the protection of CI/KR.

Figure 4-1 is a representative example of the concurrent implementation of three Federal security requirements. Please note that while this example uses the USCG as the implementing agency, it is serving as proxy for all Federal security partners.

Figure 4-1: Relationships of Maritime Security Plans per HSPD-13 and HSPD-7



- HSPD-7 establishes a national policy for Federal departments and agencies to identify and prioritize U.S. CI/KR and to protect them from terrorist attacks.
- National Security Presidential Directive (NSPD)-41/HSPD-13 is a holistic approach to Maritime Security missions comprised of the NSMS and eight supporting plans to ensure the safety and economic security of the U.S.
- The National Maritime Transportation Security Plan (NMTSP) implements ten statutory requirements of MTSA 2002 and creates a three-tier maritime security planning regime.

.

The NMTSP is the "capstone" of the three-tier MTSA security planning regime which includes: Area Maritime Security Plans (AMSPs); and vessel and facility security plans. The USCG provides guidance for the content of these plans and is responsible for inspecting and approving vessel and facility plans. AMSPs are developed with the assistance of AMSCs (comprised of Federal, State, local, and private security partners) and include a security assessment of the respective area. AMSPs are also informed by the NMTSP, which contains a National Level Maritime Risk Assessment identifying the top 29 maritime threat scenarios and 53 recommended risk reduction measures[17]. The NMTSP is aligned with the NSMS and has direct linkage by incorporating the NSPD-41/HSPD-13 Maritime Transportation System Security Recommendations by reference.

In addition, the NMTSP "Plan to re-establish Cargo Flow after a Security Incident" is aligned with the NSPD-41/HSPD-13 Maritime Infrastructure Recovery Plan (MIRP) to protect the economy of the U.S. by ensuring the continuity of maritime commerce and the MTS following a TSI. Both these plans protect a critical infrastructure system using risk-based decision making in close cooperation with State, local, tribal, and private security partners.

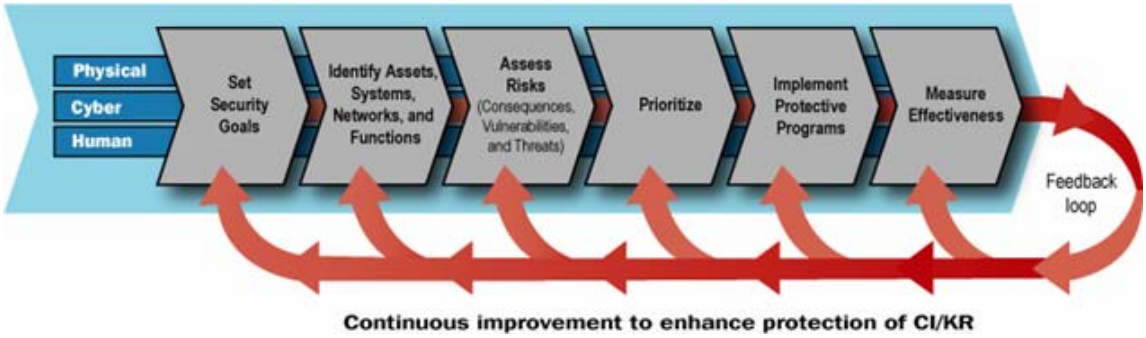
This example portrays how, within the maritime mode, a Federal agency must implement the requirements of the NIPP by implementing existing maritime security requirements. While the requirements address different aspects of maritime security, they are mutually linked and reinforce each other.

The planning and execution of these requirements with finite resources require alignment with the basic tenets of the NIPP, using Systems-Based Risk Management (SBRM) and inclusive of Federal, State, local, tribal, and private security partners to the maximum extent possible.

4.1 Approach for Achieving Sector and Modal Goals

By applying the NIPP Risk Management Framework (see figure 4-2), security partners within the maritime transportation mode will continue to establish processes for combining consequences, vulnerabilities, and threat information to produce a comprehensive systematic and rational assessment of the MTS, thereby also contributing to the overall risk management framework for the Nation. Further details are described in section 3.

Figure 4-2: NIPP Risk Management Framework



4.1.1 Assessing Risk and Prioritizing Assets and Systems

The primary tool used to assess risk to national infrastructure in the maritime domain is the MSRAM. MSRAM is a "Risk Analysis and Management for Critical Assets Protection

[17] National Maritime Transportation Security Plan (NMTSP) Section III, December 2005. The NMTSP National Maritime Risk Assessment was conducted by a multi-agency work group; the risk reduction recommendations apply to all maritime security partners.

(RAMCAP) compliant" risk analysis tool used by the USCG and other maritime industry stakeholders to analyze strategic, operational, and tactical risks within and across U.S. ports. It allows risk managers and decision makers to understand the geographic density of risk across the Nation's ports, know the profile of risk within a port, and recognize asset-specific risks to help identify maritime CI/KR assets. The tool is designed to allow a port-level user to assess risk factors associated with a target (asset) in the maritime domain in such a way that local data can be used for both local and national risk analysis needs and feeds into the overall risk management process. MSRAM is built upon the standard risk formula where Risk = Threat x Vulnerability x Consequence and also considers area-wide security measures and response capabilities. As our understanding of system-wide risks mature, MSRAM, as with other risk measurement tools, will evolve to incorporate broader system assessment data.

4.2 Programs and Initiatives

The chart below shows a representative breadth of program initiatives[18] managed by agencies throughout the maritime mode. These programs may also support other mission areas within their multi-mission agencies and respective departments.

- Goal 1: Prevent and deter acts of terrorism involving use of, or against the MTS
- Goal 2: Enhance resiliency of the MTS
- Goal 3: Maximize cost effectiveness for limited resources of the MTS

Dept./Org/Agency	MTS Program/Initiative	MTS - Goal Supported
DHS/Multiple	National Strategy for Maritime Security	1, 2, 3
DHS/Multiple	National Infrastructure Protection Plan	1, 2, 3
DHS/USCG	Operation Neptune Shield	1, 2, 3
DHS/USCG	Maritime Security Risk Assessment Management Tool	1, 2, 3
DHS/Multiple/Private Sector	Maritime Security Plans	1, 2, 3
DHS/USCG	Maritime Sentinel	1, 3
DHS/USCG/Private Sector	Information-Sharing and Analysis Center	1
DHS/USCG/Private Sector	Homeport	1, 2
DHS/Multiple/Private Sector	Maritime Security Advisory Committees	1, 2, 3
DHS/CBP	24-hour Advanced Cargo Manifest	1, 2
DHS/CBP	Container Security Initiative	1, 3
DHS/DOT/FAA/CBP	Advanced Passenger Information System	1, 3
DHS/CBP	Customs-Trade Partnership Against Terrorism	1, 3
DHS/DOD/DOS	Proliferation Security Initiative	1
DHS/USCG/CBP	Security Assessments	1
DHS/TSA/USCG	PortStep	1
DHS/TSA/USCG	Transportation Worker Identification Credential Program	1
DOJ/FBI	Maritime Liaison Agent Program	1, 2
DOJ/FBI	Joint Terrorism Task Forces	1
DOJ/FBI	InfraGard	1
DOJ/FBI	Field Intelligence Groups	1
DOT/MARAD	Maritime Security Professional Training	1
DOT/DHS/DOD	Port Readiness Committees	1, 2
DHS/USCG	Advanced Notice of Arrival (96 hours)	1
DHS/USCG	COASTWATCH	1, 2
DHS/USCG	Maritime Intelligence Fusion Center	1, 2
DHS/USCG	USCG Field Intelligence Support Team	1, 2
DHS/DOD/DOJ	Maritime Operational Threat Response	1, 3
DOT/MARAD	Safeport	1, 2

[18] A recent DHS survey identified over 260 National, Department, and component security strategies, plans, programs and regulatory requirements.

4.3 Operations Scenario

From a system of systems perspective, the MTS is a network of maritime operations that interface with shoreside operations at intermodal connections as part of overall global supply chains or domestic commercial operations. The various operations within the MTS network have components that include vessels, port facilities, waterways and waterway infrastructure, intermodal connections and users. The U.S., like many other nations, works toward maintaining a balance between safe, secure ports and facilitating trade that promotes economic growth. Through security partnerships, the principles of *detect*, *deter*, and *defend* are employed to inevitably *defeat* the growing threat of global terrorism.

The following *scenario* portrays the operational process of protection by defense systems of what could occur on a given day, in a given port:

A pilot boat drifts in 12-foot seas near the harbor entrance to a U.S. port waiting for an inbound container ship. On board that boat, in addition to the pilots, are members of the USCG's Vessel Boarding Security Team (VBST) and agents of the U.S. CBP preparing to board the ship offshore. Their mission is to ensure the ship doesn't diverge from its intended course as it enters the port and to verify the identity of the crew on board. Intelligence from international sources and the vessel's last ports of call expressed security concerns, subjecting the vessel to greater scrutiny and enhanced security measures.

At the same time the USCG's Vessel Traffic System (VTS) office monitors radar screens and computer displays. The VTS personnel analyze and assess data from Automated Identification System (AIS) signatures, radar contacts and advanced NOA in an effort to maintain MDA and to verify all vessels in or approaching the port are cleared. An 87-foot USCG patrol boat from the local USCG sector stands ready to get underway to respond to unidentified contacts or suspicious vessels.

Closer to port, the crews aboard two 25-foot armed small boats wait to escort the container ship to its berthing. These highly trained crews from the USCG's Maritime Safety and Security Teams (MSSTs) are well versed in tactics and procedures to ensure that no vessel approaches or threatens the inbound container ship.

While these boats wait to begin the escort, members of the local USCG Sector's Port State Control Teams arrive at the facility where the ship will moor. These inspection teams go aboard the ship and verify compliance with both the International Ship and Port Facility Code and Federal maritime security regulations.

During the container ship's transit through the harbor, a passenger ferry passes by. Aboard the ferry are police officers from the local port authority and MSST explosives detection canine handlers. The two agencies randomly ride the ferries to screen passengers and belongings to prevent the introduction of explosives or weapons of mass destruction (WMD) into the MTS.

This scenario depicts the furtherance of the U.S. National Maritime Anti-Terrorism Strategy of *detect, deter, defend* and *defeat*. Each aspect of the strategy is a coordination of international, national, State, and local resources and private maritime industry partners to effect a layered defense. The layered defense begins in international ports, and continues to the high seas, the littorals and finally into the ports and harbors of the U.S.

Detect. Detection of potential threats to the U.S. is the most difficult phase of the national strategy. Detection begins with the U.S. security information community overseas. The U.S. CBP's Container Security Initiative (CSI), the U.S. Department of Energy's (DOE) Megaports program and the U.S. Department of State's (DOS) Proliferation Security Initiative (PSI) strive to detect dangerous cargos, illegal immigrants, and WMD before it leaves ports where vessels engaged in international voyages are served.

The National Vessel Maritime Intelligence Center under the COASTWATCH program vets ship's crew and vessel port calls from submitted Notices of Arrival, and the CBP National Targeting Center conducts a risk-based analysis of vessel manifests for cargo, passengers and crew. Additionally, CBP has the capability to arrange for inspecting cargo overseas at 50 CSI ports, which cover 82 percent of maritime containerized import shipments. Locally, the FBI's Joint Terrorism Task Forces (JTTFs) and Field Intelligence Groups (FIGs)), along with USGC's Field Intelligence Support Teams (FISTs), collect and analyze information from field-level personnel. This information comes from national, State, and local law enforcement, port operators, vessel operators, and local citizens to identify suspicious activities occurring in and around ports, terminals, waterways, and critical infrastructure in order to disrupt the planning of a potential terrorist attack.

Deter. The object of deterrence is to make a port, ship or the nation itself a difficult target for terrorists. The USCG has led efforts for the U.S. in promoting deterrence among international trading partners, as with the creation of the International Port Security Program. International Port Security Liaison Officers (IPSLOs) are assigned to several locations world-wide to promote facility and vessel best practices.

U.S. law and regulations require port facility and vessel operators to conduct vulnerability assessments, create security plans and to implement security measures at their facilities and on their vessels to deter potential attackers. The USCG enforces regulations that impose maritime security regulations. Facility and vessel inspectors ensure training is conducted, security measures are in place and operational, and policy and procedures are being followed. A proactive deterrence method that is also being employed is "randomization." Conducting random harbor patrols, recreational and commercial vessel boardings, facility patrols, helicopter over flights, passenger and cargo screening, and increased security measures are all conducted in coordination with local law enforcement to prevent predictability and deny potential attackers the ability to complete the planning phase of a terrorist attack.

Defend. Defending our Nation against its enemies is the first and fundamental commitment of the Federal Government. If detection and deterrence have failed, a well-planned strategic and tactical defense is required. Attacks of terrorism brought into focus the need to reexamine the requirements of domestic defense. The reexamination of defense was conducted with security partners, domestically and internationally. At the national level, several changes were made in the organization of the Federal Government. In the realm of maritime security, the most significant change brought together law enforcement and consequence management agencies to create the Department of Homeland Security, where the USCG, TSA, and CBP, among others, now reside.

Within U.S. ports, commercial facility owners and operators are responsible for the safety and security of their own facilities during times of low threat. During periods of heightened threat Federal, State, and local resources may be used to augment, and at times, assume responsibility for port security. To meet this need, the USCG created 13 MSSTs that are located in strategic ports throughout the U.S. These teams consist of highly trained law enforcement boarding personnel. They have been trained to use and have access to armed patrol boats, lethal and non-lethal defensive tactics, SCUBA equipment, underwater remote-operated vehicles, radiation detection equipment, and explosive detection canines. They work in conjunction with local police Special Weapons and Tactics Teams, FBI Critical Incident Response Group tactical assets, and Navy Special Operations Forces to quickly thwart attacks and apprehend attackers.

Defeat. Defeating terrorism is a global endeavor. DHS, DOS, DOD, Department of Justice (DOJ), Department of Transportation (DOT), and other agencies work closely with other countries to develop awareness, enhance collaborative security, and provide technical assistance to increase the capabilities of partner nation maritime services for mutual benefit.

Enhancing resiliency in the MTS, to quickly recover from the effects of a TSI, will minimize the ripple effects, protect the U.S. economy, and expedite the return to normalcy.

4.4 Metrics Process

The maritime transportation mode's sector-specific program measurement scheme will leverage existing information-sharing mechanisms and partnerships to measure progress toward Transportation Sector System Goals. In general, measurement will begin with a periodic, scenario-based assessment of risk on the maritime transportation sector, followed by estimations of the percent risk reduction credited to modal implementation plans. To evaluate across the breadth of goals, it will be desirable to estimate separately, percent reductions to risk that occurs as a result of threat and vulnerability management (to track progress toward Goal 1) and consequence management (for Goal 2). Progress toward Goal 3 will be informed largely by existing Office of Management and Budget (OMB)-inspired program efficiency measures. The existing AMSC structure and MSRAM will provide the correct starting venues for conducting this measurement analysis.

4.5 Effective Practices

The MTS is a regulated environment; government and industry build efficiency into the system through the use of effective practices. Industry best practices pend formation of the SCC.

The following section describes some of the effective practices in the MTS.

4.5.1 Security Guidelines

Security guidelines are recommended activities, implemented on a voluntary basis, that enhance the security of the MTS.

- *The Container Security Initiative (CSI*). CSI is a series of bilateral, reciprocal agreements that, among other things, positions CBP personnel at selected foreign ports to pre-screen U.S.-bound containers.
- *The Customs-Trade Partnership Against Terrorism (C-TPAT).* Under CBP's layered, defense-in-depth strategy against terrorism, C-TPAT is the CBP initiative that partners, on a voluntary basis, with members of the trade community. CBP and willing members of the trade community collaborate to better secure the international supply chain to the U.S. in support of Homeland Security. C-TPAT is one of CBP's initiatives that helps the agency achieve its twin goals: security and facilitation of trade moving into the U.S.
- *America's Waterway Watch (AWW).* AWW is an outreach program, initiated by the USCG, to enhance the awareness and participation of those who live, work, or play around America's waterfront areas. Its aim is to generate more information and reports of suspicious activities. It is carried out by Active, Reserve, and Auxiliary personnel. USCG Reserve personnel concentrate on connecting with businesses and government agencies, while Auxiliarists focus on building AWW awareness among the recreational boating public.

4.5.2 Security Requirements

The Federal maritime security regime creates a comprehensive framework to enhance the security of the MTS by preventing a TSI. Some key requirements of Title 33 CFR are:

- Developed a three-tier maritime security regime:
  - 9,200 Domestic Vessel Security Plans; 3,200 Facility Security Plans
  - 43 AMSPs
  - 1 NMTSP
- Established Security Advisory Committees
  - National Maritime Security Advisory Committee (NMSAC)
  - 47 AMSCs
- Established Maritime Security (MARSEC) levels set to reflect the prevailing threat environment to the maritime elements of the national transportation system. Maritime Security Directives are instructions issued by the Commandant, USCG, or designee, mandating specific security measures for vessels and facilities. MARSEC level descriptions and representative security activities are provided below:
  - MARSEC 1: MARSEC Level 1: The level for which minimum appropriate protective security measures shall be maintained at all times. *Focus on:* Intelligence and Fusion, Harbor Patrols, Vessel Escorts, and Protection of Assets and Partnerships
  - MARSEC 2: MARSEC Level 2: The level for which appropriate additional protective security measures shall be maintained for a period of time as a result of a heightened risk of a TSI. *Increased:* Air Surveillance, Critical Infrastructure

Protection, Security Zone Enforcement, Cutters and Airborne Use of Force Deployed to Districts, Heightened Port Control, and Heightened Industry Security.

– MARSEC 3: MARSEC Level 3: The level for which specific protective security measures shall be maintained for a limited period of time when a TSI is probable or imminent, although it may be impossible to identify the specific target. *Increased:* Critical Infrastructure Protection, Maximum Port Control, Maximum Industry Security, Federal On-Scene Coordinator, Incident Command System (ICS), and WMD/ Hazard MaterialRemediation.

Customs regulations require the advance and accurate presentation of cargo declaration information before loading cargo on a vessel at the foreign port (24-hour rule). Specifically, §4.7 of the Customs Regulations (19 CFR 4.7) was amended to provide that, pursuant to 19 U.S.C. 1431(d), for any vessel subject to entry under 19 U.S.C. 1434 upon its arrival in the U.S., CBP must receive the vessel's cargo declaration from the carrier 24 hours prior to loading the cargo at the foreign port.

Vessels destined for a U.S. port or place must provide an NOA, at least 96 hours in advance. The NOA requirements are found in 33 CFR Part 60.

Signed in October 2006, the Security and Accountability for Every Port Act of 2006, or ("SAFE Port Act", Public Law 109-347) is a comprehensive maritime and cargo security bill that will strengthen port security across the Nation by establishing improved cargo screening standards, providing incentives to importers to enhance security measures and implementing a framework to ensure the successful resumption of shipping in the event of a terrorist attack, while preserving the flow of commerce. The Act establishes interagency operational centers for port security coordination and timetables and procedures for expediting the nationwide launch of the Transportation Worker Identification Credential (TWIC) program. It codifies a number of existing DHS cargo security programs, such as the CSI and the C-TPAT programs. The Act offers a plan to examine containers entering the U.S. for radiation and WMD and provides for improvements in the Automated Targeting System. The SAFE Port Act also adopts the Administration's establishment of the Domestic Nuclear Detection Office (DNDO)- the DNDO has extensive knowledge and involvement with the deployment of radiation portal monitors at ports of entry an other locations, and has been working closely with NIST to determine performance capabilities and validity of these instruments. The implementation of this Act is in progress and will be discussed in greater depth in future versions.

4.5.3 Assessment and Compliance Process

Government agencies assess compliance with maritime regulations through two main processes.

- The first of these processes is reviewing and approving regulatory requirements backed by on-site inspections and spot checks. The USCG publishes minimum required contents for MTSA required vessel and facility security plans. These plans are reviewed and approved by the USCG; compliance with these requirements is assessed during on-site inspections.
- The second method of compliance assessment is the concept of layered defense. No single security program is a stand-alone program, but each is part of a layered security regime. The scenario presented earlier highlighted the effects of this layering as multiple programs continuously assess cargo and persons being transported on the MTS. Cargo being shipped to the U.S. must be reported to customs 24 hours prior to lading. A C-TPAT partner's cargo shipping from a CSI port will still be reanalyzed by the National Targeting Center and the conveyance will make an NOA 96 hours before arriving in a

U.S. port. Upon arrival, the conveyance is subject to boarding inspections and the cargo/personnel will need to clear customs before entering the U.S. through an intermodal gateway.

4.5.4 Training and Exercises; Government-Effective Practice

Training is an integral part of implementing protective programs, and is conducted regularly by security partners. Exercises provide an opportunity to identify gaps in existing implementation plans while improving familiarity with the contents and competence in execution. While there are some regulatory requirements for training and exercises, other non-required training and exercise venues offer opportunities for collaboration among security partners. Scenario-based training can offer a system's perspective in the protection of critical infrastructure; participation in training and exercises occurs from the National to the local levels. Because no overarching training and exercise plan exists for the Nation, agencies will continue to meet training and exercise requirements for their individual agencies and seek to identify opportunities to incorporate modal security partners. The Sector Partnership Model provides forums to identify future opportunities to conduct both training and exercises, and to gain efficiencies and enhance knowledge management.

4.6 Grant Programs

As a component of the Infrastructure Protection Program (IPP), the Port Security Grants Program (PSGP) seeks to assist the Nation's ports in obtaining the resources and capabilities required to support the National Preparedness Goal and the associated National Priorities. Through its focus on port-wide risk management planning and domain awareness in the port environment, the PSGP directly addresses six of the seven National Priorities:

1. Expanding regional collaboration
2. Implementing the National Incident Management System and the NRP
3. Implementing the NIPP
4. Strengthening information-sharing and collaboration capabilities
5. Enhancing interoperable communications capabilities
6. Strengthening Chemical, Biological, Radiological, Nuclear, or (High-Yield) Explosive (CBRNE) detection and response capabilities.

In addition, the PSGP also supports strengthening emergency operations planning and citizen protection capabilities, and assists in addressing security priorities specific to the port environment. The PSGP uses a port-wide risk management program as part of urban area and State efforts. The process is patterned after the risk management framework articulated in the NIPP. Adopting a deliberate risk management planning process enables the FMSC and AMSC to make security enhancement decisions in the context of strategic security goals, supported by clear, measurable objectives. This process allows port area security needs to be integrated into the broader national risk management framework of the NIPP, into the regional planning construct that forms the core of the Urban Area Security Initiative (UASI) program, and into statewide initiatives. Similar to MTSA, the SAFE Port Act of 2006 requires that each grant be used to supplement and support, in a consistent and coordinated manner, the applicable Area Maritime Transportation Security Plan. Each grant is also coordinated with any applicable State or urban area homeland security plan. The Act also states that the PSGP must take into account national economic, energy, and strategic defense concerns based on the most current risk assessments available.

4.7 Way Forward

This modal implementation plan is the result of a collaborative effort between security partners in both the private sector and public sector of the MTS. This plan captures how the maritime transportation mode as a component of the Transportation Systems Sector fits within the goals of the Transportation Systems Sector and how it contributes to the outcome of achieving these goals.

The MTS continues to evolve and respond to changes. The resultant cooperation and collaboration between and among existing and newly identified security partners continues to increase. From a systems perspective, communication is critical to the successful implementation of this plan, as well as the related family of plans. As NIPP partnerships evolve within the Transportation Systems Sector and the maritime transportation mode, so will a more mature risk-based methodology approach that will assist in the future identification and prioritization of resources for CI/KR protection.

The Departments of Homeland Security, Justice, Transportation, Commerce, Interior, and Defense all have a stake in MTS security. While the USCG is designated as the lead DHS agency for maritime homeland security and the SSA for the maritime transportation mode, securing the MTS requires a team effort at all levels. The SSA is positioned to enable, assist and collaborate with security partners in implementing, executing and sustaining of the processes and procedures necessary to secure the MTS in support of HSPD-7, HSPD-13, the NIPP, and other related plans.

The MDA Implementation Team, an interagency body of senior executives, is producing a Concept of Operations and an Investment Strategy that provides a structure under which maritime stakeholders within the Federal government will align efforts to enhance MDA. The associated processes will be characterized by spiral development; as the relationships and partnerships in the MTS evolve, so will the information-sharing processes for MDA. MDA will evolve to include commercial, private sector, and international partners. These adaptable processes will adjust to the changing nature of the threats and associated risks as well as to enhancements in supporting technologies.

Protecting and ensuring the continuity of U.S. maritime CI/KR is essential to the Nation's security, public health and safety, maritime commerce vitality, and the maritime sector way of life. Terrorist attacks on maritime CI/KR and other manmade or natural disasters could significantly disrupt the functioning of government and private sector businesses alike, and produce cascading effects far beyond the affected ports, waterways, and coastal areas of the actual incident location. Terrorist attacks using components of the MTS CI/KR as WMD or disruption could have even more devastating physical, psychological, and economic consequences.

5 Program Management

Although the MTS and efforts to protect CI/KR of the U.S. within the maritime domain are mature, the coordinating mechanisms stemming from the requirements of the NIPP are more recent. The maritime transportation mode will continue to evolve to meet these new requirements.

5.1 Coordinating Mechanisms

The SSA for the maritime transportation mode will continue to perform a leadership role alongside other SSA's as identified in the NIPP, continue to serve on the TSGCC, and continue to chair the MMGCC. The SSA will use the MMGCC to promote cooperative efforts among security partners to ensure the modal implementation plan is updated using sanctioned communications processes and the Sector Partnership Model wherever possible.

In March 2006, the MMGCC stood up as a subsector of the Transportation Sector Government Coordinating Council (Transportation Sector GCC). Primary membership as of November 2006 consists of representatives from:

- U.S. Department of Homeland Security
  - Transportation Security Administration
  - Customs and Border Protection
  - DHS Office of Policy
  - DHS Office of Infrastructure Protection
- U.S. Department of Transportation
  - DOT Office of Policy
  - Maritime Administration
- U.S. Department of Defense
  - DOD Office of Transportation Policy
  - U.S. Army Corps of Engineers
- U.S. Department of Commerce
  - Transport and Security Office of Service Industries
- U.S. Department of Justice
  - Federal Bureau of Investigation

The responsibilities of the MMGCC are derived from the NIPP and the charter of the Transportation Sector GCC. Member agencies and representatives of the MMGCC may also participate in other HSPD-7 designated CI/KR sectors and transportation modes.

The SSA and other Federal agencies within the maritime transportation mode have a long history of partnering with industry and the private sector to meet various safety and security goals. The MMSCC will enable private sector security coordination and is currently under development.

5.2 Work Plan

The MMGCC will form a work group to develop a 2- to 5-year work plan; the Sector Partnership Model will be used whenever possible. This work plan may consider the following:

- Identify forums and/or existing committees where synergy may be created by information-sharing and collaboration with the MMGCC
- Examine and expand representation on Transportation Sector GCC work groups, as applicable
- Encourage maritime transportation mode representation on the Transportation SCC
- Expand MSRAM capabilities
- Contribute to sector CI/KR Annual Report
- Develop and define future roles and responsibilities of the MMGCC
- Identify methods and potential measures to be undertaken by government and/or the private sector to increase the efficiency of MTS infrastructure recovery and resumption of maritime trade following a significant incident