NATIONAL CONCEPT OF OPERATIONS FOR

MARITIME DOMAIN AWARENESS

December 2007

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

EXECUTIVE SUMMARY

No one country, Department, or Agency holds all of the authorities and capabilities to achieve effective Maritime Domain Awareness. MDA can only be achieved through a collaborative network of partners drawing upon their cumulative authorities and capabilities. It is only through unity of effort that the security, safety, economic and environmental objectives associated with MDA can be achieved.

This Maritime Domain Awareness (MDA) Concept of Operations (CONOPS) provides a foundation for developing interagency and agency-specific policies, processes, procedures, and organizational relationships to align activities that contribute to achieving MDA. This initial spiral is primarily interagency focused, providing a federal approach to developing maritime domain awareness at home and abroad in support of the security, safety, economy, and environment of the United States. Many of the concepts and ideas expressed in this document are also applicable in working with local, state, tribal, international and private sector partners. Achieving MDA depends on the ability to monitor activities in such a way that trends can be identified and anomalies detected. The desired state is transparency in the maritime domain.

This document has two purposes. First, it is intended to execute the *National Plan to Achieve Maritime Domain Awareness* (MDA Plan) in support of the National Strategy for Maritime security and National Security Presidential Directive-41 / Homeland Security Presidential Directive-13 and help create an effective, on-going National MDA Enterprise. Second, it seeks to provide the members and leadership of that enterprise the benefit of understanding gained by inter-departmental work groups over a period of three years. It is intended to be strategic in nature so as to permit flexibility in addressing agency-specific needs.

Maritime Domain Awareness (MDA) is the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States.[1] However, this does not mean that knowing everything everywhere in the maritime domain is a requirement to achieving MDA. This CONOPS develops a framework for describing what needs to be known, as well as where or when that information needs to be available in order to guide the systematic development of requisite capabilities. It establishes a construct for categorizing types of information and prioritizing areas in the world where information must be collected.

Conceptually, MDA is the integration of Global Maritime Intelligence and Global Maritime Situational Awareness. Global Maritime Intelligence is the product of legacy, as well as changing intelligence capabilities, policies and operational relationships used to integrate all available data, information, and intelligence in order to identify, locate, and track potential maritime threats.[2] Global Maritime Situational Awareness results from the persistent monitoring[3] of maritime activities in such a way that trends and anomalies can be identified.

---

[1] National Plan to Achieve Maritime Domain Awareness

[2] Global Maritime Intelligence Integration Plan

[3] As defined in the *National Plan to Achieve Maritime Domain Awareness*; "Persistently Monitor" refers to an ability to persistently monitor anywhere on the globe but is not meant to imply the ability to simultaneously persistently monitor the entire globe.

This CONOPS describes an open net-centric architecture for information sharing throughout the Global Maritime Community of Interest (GMCOI) and across all of the associated MDA pillars (vessels, cargo, people, and infrastructure). An MDA architecture founded upon net-centric principles will provide a secure, collaborative, information-sharing environment and unprecedented access to decision-quality information. A fundamental attribute of a net-centric environment is the ability for any consumer of information to get the information that is needed, when it is needed. This construct establishes an environment in which each data provider publishes their data for consumers to discover and retrieve, based on appropriate permissions. This approach effectively separates the data from the underlying application or system making it available to a wide range of qualified users for a wide range of uses. The Enterprise will have multi-level security protocols with cross-domain information sharing allowing information to flow between classification domains, and be automatically sanitized when flowing from higher to lower levels. MDA key components, situational awareness and intelligence information will need to be combined and presented in a flexible operating picture. Through a User Defined Operating Picture (UDOP), users will eventually monitor MDA pillars, other areas of interest and have access to all relevant databases. Users will then perform collection, analysis, and dissemination. This collaborative concept of a UDOP is founded upon a net-centric services-oriented architecture.

Another key aspect of this CONOPS is interagency governance to coordinate and unify efforts across a broad range of federal, state, local, tribal, private sector and international partners. An interagency MDA governance structure must provide sufficient direction in developing policy and standards to guide individual agencies and partners in sharing information and intelligence and working together to ensure continued alignment of efforts to achieve national MDA goals. This CONOPS establishes a structure to align the efforts of the Directors of the Global Maritime Community of Interest Intelligence Enterprise and Global Maritime Situational Awareness Enterprise through a Maritime Domain Awareness Stakeholder Board. The staff for each Governance component will consist of appropriate subject matter experts from cognizant agencies. This governance organization will have policy development, guidance and coordinating responsibilities, but will not exercise operational control of resources or assets that contribute to MDA. The authorities of federal departments and agencies, to include the chain of command for military forces and tasking of civil assets, will not be altered or impaired by this organization.

Recognizing that there are numerous existing facilities that already contribute greatly to the nation's MDA, this document proposes the designation of Enterprise Hubs. Designation as an Enterprise Hub confers two primary responsibilities; coordinate information flow for the respective subject area both domestically and internationally, and facilitate the sharing of related intelligence, information and data within and across Hubs and throughout the maritime community of interest. Enterprise Hubs for Vessels, Cargo, People, Infrastructure and Architecture are proposed from existing organizations that already possess subject matter expertise, a preponderance of the requisite authorities, and knowledge of associated capabilities and procedures. These Enterprise Hubs will be linked to intelligence and information providers and able to share pertinent data throughout the GMCOI. In the future these Hubs will grow into a virtual analysis and fusion network as technology capabilities increase. A lead agency for development of the MDA information architecture is also proposed.

The MDA CONOPS is an overarching document applicable to all federal stakeholder agencies under which individual departments and agencies can develop specific operational guidance, tactics, techniques and procedures. This document will continue to evolve. Follow-on iterations will address intelligence and information sharing with state, local, tribal, private sector and international stakeholders. Achieving the desired capabilities in this and subsequent spirals requires continued investment of our Nation's intellectual, technological, human and financial resources, as well as a partnership with all nations and international maritime entities.

Table of Contents

This page intentionally left blank.

1. Purpose

This document describes a Concept of Operations (CONOPS) to execute the *National Plan to Achieve Maritime Domain Awareness* (MDA Plan). It is part of a comprehensive national effort to enhance the safety, security, economy and environment of the United States by deterring and preventing hostile or illegal acts within the maritime domain.

The current capability of the United States to create awareness to mitigate maritime security risks and respond to maritime threats is incomplete. Today, MDA is achieved through a mix of established arrangements and uncoordinated employment of non-standard processes on a routine and as-needed basis. These varied processes, data systems, and sharing arrangements among stakeholders are insufficient to achieve the level of MDA required to support a proactive maritime security strategy. Further, existing organizational relationships, authorities and responsibilities do not provide overall accountability for awareness outcomes.

This CONOPS is written to execute the *National Plan to Achieve Maritime Domain Awareness* by establishing an on-going National MDA organizational structure. It is intended to meet the following objectives:

- describe the interagency desired state of MDA: An environment in which the GMCOI embraces and achieves the common objective of obtaining and sharing information as a mechanism to increase safety, security, and economic prosperity in the maritime domain;
- improve MDA planning and execution at all levels by establishing an interagency perspective for partnering and coordination efforts;
- provide an initial framework that enhances MDA and serves as an input to capability development;
- provide a foundation for a process to identify and close current MDA-related capability gaps and measure progress;
- provide sufficient detail regarding desired capabilities to form the basis for development of an interagency MDA investment strategy;
- describe information architectures needed to share data, intelligence and information in the Global Maritime Community of Interest (GMCOI);[4] and
- recommend changes to MDA-related policies and statutes.

2. Scope

This initial version of the CONOPS is applicable to federal agencies within the GMCOI, and informs other GMCOI stakeholders. Subsequent iterations will expand the scope to include

[4] GMCOI includes, among other interests, the federal, state, local and tribal departments and agencies with responsibilities in the maritime domain. Because certain risks and interests are common to government, business, and citizen alike, community membership also includes public, private and commercial stakeholders, as well as foreign governments and international stakeholders. Page 1, MDA Plan.

other levels of government, as well as international partners and the private sector as the concept of MDA evolves.

The MDA Plan and the *Global Maritime Intelligence Integration* (GMII) *Plan* are mutually supportive and both are key enablers for the other supporting plans under the *National Strategy for Maritime Security* (NSMS),[5] including response under the *Maritime Operational Threat Response* (MOTR) Plan.

This CONOPS was developed with full consideration of existing programs and current initiatives affecting maritime security. A number of these programs have been in place for many years, and many more are being developed concurrently with this CONOPS. For example, the Security and Accountability for Every Port Act or the SAFE Port Act became Public Law No: 109-347 on October 13, 2006. Appendix B contains a more complete listing of related documents, laws and acts.

2.1 *Key Definitions*[6]

Maritime Domain is 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.[7]

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.[8]

Global Maritime Intelligence (GMI) is the product of legacy as well as changing intelligence capabilities, policies and operational relationships used to integrate all available data, information and intelligence in order to identify, locate, and track potential threats to maritime interests. It provides accurate, relevant and collaborated maritime threat information to operational and law enforcement entities, supporting a variety of tactical, operational, and strategic requirements.[9]

Global Maritime Situational Awareness (GMSA) is the comprehensive fusion of data from every agency and by every nation to improve knowledge of the maritime domain. GMSA results from persistent monitoring of maritime activities in such a way that trends can be identified and anomalies detected. It is a layered picture of the current state and trends that includes information pertaining to MDA pillars (vessels, cargo, people and infrastructure) and related economic and environmental issues.

---

[5] Other plans include the *Maritime Transportation System Security* (MTSS) *Recommendations*, *Maritime Commerce Security Plan* (MCS), *Maritime Infrastructure Recovery Plan* (MIRP) *International Outreach and Coordination Strategy* (IO), and *Domestic Outreach Plan* (DO).

[6] A comprehensive list of definitions and acronyms is contained in Appendix A. Appendix B contains a list of maritime security and information sharing references.

[7] *National Plan to Achieve Maritime Domain Awareness*

[8] *National Plan to Achieve Maritime Domain Awareness*

[9] *Global Maritime Intelligence Integration Plan*

2.2 *MDA*

As stated previously, effective MDA can only be achieved through the integration of Global Maritime Intelligence (GMI) and GMSA (MDA = GMI + GMSA). However, an important distinction must be made between the responsibilities of the maritime agencies developing GMI and the responsibilities of those maritime stakeholders providing GMSA. The complementary and interactive qualities of GMI and GMSA will be repeated throughout this CONOPS to emphasize the foundational dependence upon this partnership. This CONOPS seeks to build synergy between intelligence and situational awareness. GMSA and GMII organizations must exist as symbiotically interdependent organizations seeking to integrate intelligence, information, situational awareness and threat information.

Stakeholders providing both GMI and GMSA are involved in the collection, analysis, fusion and dissemination of information and intelligence to decision-makers. While intelligence efforts seek to identify threats and provide cueing, situational awareness focuses on persistent monitoring of maritime activities allowing trends to be identified and anomalies detected. The distinction is generally identifiable in that GMII is responsible for: 1) all-source intelligence analysis 2) responding to identified intelligence needs from decision-makers, 3) focusing on predictive threat warning, and 4) providing detailed cueing that characterizes the evolving threat. By contrast, GMSA provides a comprehensive view of the MDA pillars, the synthesized whole characterizing "maritime normal."

Only when GMI and GMSA are integrated together will decision-makers have the effective understanding that defines MDA. It is the intent of this CONOPS to ensure that the capabilities of GMI and GMSA are fully integrated and coordinated, especially as they relate to the functionality of supporting information management systems.

2.3 *GMI*

GMI is the product of intelligence capabilities, policies and operational relationships used to integrate available data, information and intelligence in order to identify, locate, and track potential threats to the national security and maritime interests of the United States and partner nations. GMI's primary function is to identify the cargo, vessels, and people that pose a potential threat to maritime interests. Per the GMII Plan, strategic analysis and intelligence integration of maritime activity will be integrated with GMSA to help achieve MDA.

2.4 *GMSA*

GMSA is the persistent monitoring of maritime activities in such a way that trends can be identified and anomalies detected. It is the product of a comprehensive fusion of data from every agency and by every nation with knowledge of the maritime domain. It is a layered, highly detailed picture of the current state and trends that includes information pertaining to the MDA pillars, the environment and financial transactions. The GMSA picture can identify anomalies in the daily flow of maritime commerce, a complimentary process to the threat cueing provided by GMII.

3. Planning Assumptions

In addition to assumptions in the *National Strategy for Maritime Security* and the *National Plan to Achieve MDA*, the following assumptions are used in the development of this document:

- The proposed governing organization will be approved and implemented;
- There will be a continuing need to collaborate across the interagency and among other stakeholders to accommodate virtual collaboration across the various MDA pillars;
- The MDA CONOPS and subsequent iterations will accommodate determination of requirements and priorities for a wide variety of stakeholders;
- A legal framework will exist to allow stakeholders to share maritime-related data to the greatest extent possible;
- Stakeholders will collaborate in networking existing capabilities into cooperative systems;
- All stakeholders are sensitive to fiscal and budget issues in the implementation of this CONOPS and in the development of new capabilities;
- Technology, including collection sensors, fusion and analysis techniques and dissemination tools will advance, enabling improvements in future capability;
- The dynamic between security constraints and economic interests will influence information sharing and security actions;
- MDA is a global project that requires the participation of foreign partners; and
- Technology will enable sharing of maritime-related data through emphasis on interoperability, standards, open architecture, re-use of information (input once, access many times) and collaborative processes.

4. Problem

In order to gain an effective understanding of the maritime domain, information and intelligence must be gathered and shared across numerous stakeholder agencies. However, numerous obstacles impede the ability to share intelligence and information that is necessary to achieve MDA including:

- Databases that are not adequately connected in a way that allows the identification of information gaps or redundancies;
- The inabilities to persistently monitor critical areas, associate data with detected targets, and otherwise create situational awareness;
- Incompatible and proprietary operating systems and organizations;
- Lack of trusted partnerships and a cultural propensity not to share information and intelligence inhibiting effective knowledge management;
- Real and incorrectly perceived policy restrictions on sharing data. Few statutory limitations exist to prevent sharing of specific information. Most restrictions are based on internal policy and perceived sharing constraints;
- Limited interagency communications, connectivity and interoperability exacerbated by multiple classification systems that lack seamless cross-security domain solutions (e.g., For Official Use Only, Sensitive but Unclassified, Sensitive Security Information, Law Enforcement Sensitive);

- Limited interagency awareness of complementary mission sets that impede development of a true community of interest; and
- Limited understanding of data contained in proprietary and government systems.

5. Desired State

The desired state is an environment where federal, state, local, tribal, private sector and international partners can embrace and achieve the common objective of obtaining and sharing information as a mechanism to increase safety, security and economic prosperity in the maritime domain and have the supporting architecture to do so.

Achieving MDA depends on the ability to monitor activities in such a way that trends can be identified and anomalies detected. Data alone is insufficient. Data must be collected, fused and analyzed with the assistance of computer data integration and analysis algorithms. These automated fusion and analysis tools will allow handling vast, disparate data streams, so that operational decision makers can anticipate threats and take the initiative to defeat them. The following objectives constitute the MDA Essential Task List from the MDA Plan. These essential tasks will identify and guide development of operational capabilities and requirements:

- persistently monitor in the global maritime domain
  - vessels and craft,
  - cargo,
  - vessel crews and passengers[10], and
  - all identified areas of interest;
- access and maintain data on vessels, facilities, and infrastructure;
- collect, fuse, analyze, and disseminate information to decision makers to facilitate effective understanding; and
- access, develop and maintain data on MDA-related mission performance.

Achieving these objectives enables threat identification and facilitates effective decision-making. To this end, the CONOPS lays the ground work for:

- MDA governance that effectively develops national MDA policies and supporting strategies to
  - develop GMSA,
  - integrate GMI and GMSA,
  - develop future versions of this CONOPS, and
  - help guide execution of the national interagency MDA investment strategy;

[10] See Appendix C-3 for the inclusive definition of "people" in the maritime domain.

- policies and procedures for collaboration and information and intelligence sharing among stakeholder agencies;
- optimized flow of intelligence and information among all domains to include the private sector and international/coalition partners;
- an open-system architecture that facilitates accurate, timely and inter-operable information and intelligence sharing and promotes collaboration among the GMCOI;
- fulfilled information needs of MOTR agencies and other decision makers;
- access to all information and intelligence commensurate with appropriate security clearance protocols and authorities;
- a global, network-based awareness arising from cooperative collection, analysis (including anomaly detection, pattern analysis, and knowledge-discovery in databases), fusion and dissemination of maritime data, information and intelligence;
- near real-time, dynamically tailored, network-centric information shared by US federal agencies and available to all state, local and tribal agencies and international partners with maritime interests and responsibilities;
- automated fusion capabilities that integrate into net-centric architecture;
- a framework for data management and archiving to support fusing of information and intelligence data;
- a framework for identifying and prioritizing capability development for collection, analysis, fusion and dissemination needed to address gaps, improve performance and implementation strategies;
- Processes for integrating capability across disparate organizations and cultures including training, exercise and experimentation; and
- Employment of appropriate measures of effectiveness to consistently evaluate and improve GMSA and GMII performance.

6. Creating MDA

MDA is not a particular mission or task, but rather the result of the proper integration of a diverse set of capabilities, which provide decision makers with an effective understanding of the maritime domain. This effective understanding facilitates the decision making process and enables operational response.

Persistent monitoring requires integrated management of a diverse set of collection and processing capabilities, operated to detect and understand activities of interest associated with the MDA pillars, and related economic and environmental issues with sufficient endurance, repeatability, and quality to enhance awareness and influence decisions. It does not imply the ability to simultaneously monitor all maritime activities worldwide, but rather to monitor activities in such a way that trends and anomalies can be identified. While methodologies vary across the GMCOI, tasks that support the creation of MDA can be grouped into four broad categories. These tasks are not necessarily performed sequentially, but are part of an iterative process, the exact nature of which varies by situation. Creating MDA involves collection,

fusion, analysis and dissemination of data and information. This data must be developed into discoverable information and disseminated to decision makers. Finally, this data must be archived and maintained in a manner to allow trend analysis, anomaly detection and future study.

The expected day-to-day MDA operations will generate incredibly large amounts of data and information. Effective fusion and analysis will require a proactive and very robust approach to Knowledge Management (KM). KM is a concept in which an enterprise or organization consciously and comprehensively gathers, organizes, shares, and analyzes its knowledge in terms of resources, documents, and people skills. In other words, MDA KM allows capturing, organizing, and storing knowledge and experiences of individual workers and groups within the GMCOI and readily makes this information available for seamless information sharing to others.

6.1 *Monitoring and Collection*

Monitoring and collection involve gathering data and information in any manner and from any source. Data and information may come from routine surveillance operations and sensors, cued intelligence sensors and sources, open source publications, archived data bases, or reports from members of the maritime community (e.g. first responders, shipping industry, etc.). Collection will involve cooperation between collection assets operated by the intelligence community and those operated by other non-intelligence organizations. This will require cooperation between the GMII Director and the GMSA Director to manage the tasking for the intelligence assets.

6.2 *Fusion & Analysis*

Data fusion and analysis is the process of combining data or information to determine what significant and actionable knowledge is present in all available data. This can mean estimating or predicting entity status, determining relationships, assessing situations, or assessing potential vulnerabilities, threats, and consequences. For MDA purposes, an entity may be a person, physical object, concept, relationship, or an event. An internationally agreed upon data model and reference standards, including computer-assisted analysis tools, need to be established to enable interoperability between diverse systems.

Data fusion is data association and knowledge-discovery. Data association uses commensurate information in the data to determine which data belongs together. It is the definition and calculation of a closeness metric on which the assignment of data or semantic reports to customers will be decided. Knowledge-discovery in databases is the process of discovering previously unrecognized patterns in data. The objective is to use these tools to convert data and information into useable knowledge for the decision maker.

Analysis is the process of examining collected data in detail to detect an activity of interest, operating patterns and anomalies, capability and intent. MDA is the integration of intelligence and information within the broader context of associated situational awareness (SA). The goal is to provide the necessary level of awareness to the end-users of the information about specific MDA pillars.

6.3 *Dissemination*

Dissemination is the process of getting the right information to the right users. For MDA, the desired state is to provide pertinent data, products, alerts, and warnings to support decision makers, analysts, and responders within the GMCOI. The dissemination of data, products, alerts, and warnings is achieved through a web-enabled, net-centric architecture that permits GMCOI

access to pertinent database information in a timely fashion. The desired state is also to get the needed intelligence and information to the decision makers in time for them to act. MDA information, intelligence, data, products, and services will be the sources for developing GMCOI User-Defined Operational Pictures (UDOPs). The characteristics of this global network will include multi-level security and access, allowing users to pull or subscribe to desired information and data from widely disparate data repositories, and to push or publish information, alerts, and warnings as warranted.

6.4 *Archiving & Maintaining*

Archiving and maintaining includes retention and retrieval of historic data and continuity of operations capability. These functions are essential for effective MDA as they allow association of historic data with current monitoring and collection. It includes ensuring compliance with information assurance standards and assessing data quality, integrity, and pedigree. Information archives also support rapid restoration of awareness after natural disaster, national emergencies, or successful attack.

7. Information Architecture

Information architecture to support MDA founded upon net-centric principles will provide a secure, collaborative, information-sharing environment and unprecedented access to decision-quality information. A fundamental net-centric attribute is the ability for any consumer to get information that is needed, when it is needed. A net-centric environment is one in which each data provider exposes data for consumers to discover and retrieve. This approach effectively separates the data from the underlying application or system making it available to a wide range of users for a wide range of uses. The Enterprise will have multi-level security protocols and permissions. Cross-domain sharing will enable information to flow between classification levels, with automatic sanitization when it passes from a higher to lower classification.

The concept of a Services-Oriented Architecture (SOA) allows access to valuable data and applications across any particular community of interest. It provides flexibility to address unexpected data requirements. The SOA also allows the original data stewards to control their own data, both in terms access requirements and data integrity. It allows agencies to retain the investment they have made in their existing systems. It also uses internet technology, which is user-friendly and readily understood. The concept of a User Defined Operational Picture (UDOP) is founded upon a services-oriented architecture. One example of an SOA is the DHS SOA Information Sharing Framework, which has been approved as the SOA standard for Department-wide internal use.

A UDOP is a picture of the maritime situation tailored by an individual user from a common pool of data using processing methods of their choosing, whereas a common operational picture (COP) implies uniformity in the source and display of data. A SOA enabled UDOP allows each user to define the sources of data and the “look and feel” of their own picture display. Each user will be looking at a unique, but accurate, picture of the maritime domain that serves their mission needs and interests. In this way, all members of the GMCOI can use MDA to their best advantage, and leverage their expertise, experience, and authorities in the cause of maritime security, defense, safety, and stewardship.

7.1 *Desired Architecture*

While the goal in the near term is to establish information exchange processes and practices, the objective for the desired state is to develop and implement an integrated net-centric enterprise. The enterprise network will depend upon four product lines:

- a services-oriented architecture foundation that provides a structure for interoperable computing. The core services include security and information assurance, service discovery, enterprise services management, machine-to-machine messaging, people and device discovery, mediation and metadata registry services;
- collaboration that enables synchronous communications and file sharing among users. These services include session management, presence and awareness, audio collaboration, video collaboration, text collaboration, application sharing, application broadcasting, and virtual space;
- content discovery and delivery that provides common specifications to expose, search, retrieve and deliver information across the enterprise; and
- portal services that provide personalized, user-defined, web-enabled presentation and offer secure access to the enterprise.

Users will be granted access parameters dependent on roles, responsibilities and authorities and then enjoy unfettered use of a range of products and services available within the multi-level security enterprise. An initial set of common core services available to the GMCOI is envisioned to include:

- discovery services that provide processes to identify information content or services that exploit metadata descriptions of Information Technology resources stored in directories, registries and catalogs, to include search engines;
- collaboration services that allow users to work together and jointly use selected capabilities on the network;
- mediation services that help broker, translate, aggregate, fuse or integrate data;
- messaging services that provide the ability to exchange information among users or applications on the enterprise infrastructure;
- platform services that provides infrastructure to host and organize distributed on-line processing;
- storage services that provide physical and virtual places to host data on the network with varying degrees of persistence, such as archiving, continuity of operations and content staging;
- security services that provide capabilities to address information assurance standards, operational availability, network vulnerabilities, and system security; and
- enterprise management services that provide end-to-end performance monitoring, configuration management and problem detection and resolution, and enterprise resource accounting and addressing for users, systems, and devices.

In the event of any one of a wide range of disruptive events, the system must be maintained at a high level of readiness. A robust continuity of operations capability is vital to response, recovery, and risk mitigation. This continuity of operations must be capable of implementation both with and without warning and must be able to recover quickly and minimize down time. These core services should be designed to facilitate exchanges with parallel efforts to MDA (e.g., Air Domain Awareness (ADA)) to facilitate overlapping interests in tracking the movement of cargo and people through the global transportation system.

8. Governance

No one department or agency holds all of the authorities and capabilities necessary to achieve effective MDA. MDA can only be achieved through a collaborative network of partners that draw upon their cumulative authorities and capabilities. It is only through unity of effort that the security, safety, economic and environmental aspects associated MDA objectives be achieved.

A key goal of this CONOPS is the development of a federal interagency leadership structure for achieving MDA. Achieving MDA will require coordinated focus and unity of effort across a broad range of federal, state, local, tribal, private sector and international partners. However, clear government-wide policy and guidelines regarding the sharing of intelligence and information have not been fully implemented.

An MDA Governance Organization is needed to ensure a shared perspective across the GMCOI, including balancing the equities of civil, military, private sector and international stakeholders. The governance organization will have MDA policy and oversight roles and maintain a perspective on how well those policies enable activities that enhance MDA. The governance organization will be responsible for encouraging and monitoring the implementation of effective national policies and procedures to achieve MDA.

As previously discussed, MDA is the integration of GMI and GMSA (MDA = GMI + GMSA). While intelligence efforts seek to identify threats and provide cueing, situational awareness focuses on persistent monitoring of maritime activities allowing trends to be identified and anomalies detected. The Governance organization is designed to develop synergy between intelligence and situational awareness.

The structural and functional aspects of the GMII Enterprise and the GMSA Enterprise are described in the following sections. This CONOPS calls for a MDA Stakeholder Board that will serve to coordinate, integrate and reconcile the efforts of GMII Enterprise and GMSA Enterprise. The GMII Enterprise, and GMSA Enterprise Directors' policy development, guidance and coordination responsibilities will not impair or otherwise circumvent the authorities of federal departments or agencies, nor the chain of command for military forces, nor tasking of civil assets.

The overall governance organization consists of a MDA Stakeholder Board, co-chaired by the Director of GMII Enterprise and the Director of GMSA Enterprise, with supporting staffs. The MDA Stakeholder Board should include representatives from a broad cross-section of agencies, (e.g., Department of Energy's National Nuclear Security Administration, Customs and Border Protection, Federal Bureau of Investigation, Immigration and Customs Enforcement, the Intelligence Community, U.S. Coast Guard, and U.S. Navy) in order to ensure appropriate equities are represented and all information and intelligence sharing opportunities are exploited

and evaluated as a means to achieve MDA. The Director of GMSA Enterprise will fill the role of MDA Stakeholder Board executive secretary. Coordination between GMI and GMSA at all levels from the Stakeholder Board to individual action officers is critical to success.

8.1 *Governance Characteristics*

Leadership

An effective information sharing environment is not sustainable if trust among all of the stakeholders is not developed and maintained. Along with developing trust, the governance organization must have the ability to effectively collaborate with, and if necessary represent the equities of, a wide variety of maritime stakeholders at all ends of the MDA spectrum from providers to users and responders.

Policy Guidance

The MDA governance organization must provide clear intelligence and information sharing policies, protocols and standards to allow, to the maximum extent possible, individual agencies and partners to collaborate fully and broadly share information, while protecting civil liberties.

Oversight and Accountability

Participants in the GMCOI need to know that their data will be protected. The MDA governance will implement oversight and accountability measures. Likewise, policy-makers need to have the confidence that the statutes and policies governing the sharing of information are being implemented, followed, and enforced. Perhaps most important, the public needs to know that the information sharing environment is protecting national security in accordance with existing laws, policies, traditional civil liberties, and is subject to oversight and enforcement.

Coordination

The Governance Organization must be able to coordinate existing organizations' authorities, responsibilities, interagency relationships and subject matter expertise to ensure increased and continued national effectiveness across the full range of maritime missions and activities.

Additional Characteristics

Additional characteristics of the MDA Governance Organization include:

- appropriately positioned within the federal government to present legal and policy change recommendations to appropriate bodies;
- representation from all primary federal MDA stakeholder agencies;
- access to sufficient information technology expertise to evaluate and recommend modifications to existing architectures and evaluate new technologies to facilitate the collection, analysis, fusion and dissemination of intelligence and information, while also providing for the safeguarding of the data; and
- access to legal and civil liberties protection review and expertise.

8.2 *Maritime Domain Awareness Stakeholder Board*

The Maritime Domain Awareness Stakeholder Board will be responsible for policy coordination, alignment, synergy and issue resolution between the GMII Enterprise and the GMSA Enterprise.

The MDA Stakeholder Board will be co-chaired by the Director of GMII Enterprise and the Director of GMSA Enterprise with representation from maritime stakeholder agencies and those agencies responsible for the eight plans that support the National Strategy for Maritime Security. The Stakeholder Board, through the co-chairs, will serve as a conduit to the Maritime Security Policy Coordinating Committee (MSPCC). The co-chairs are responsible for promoting unity of effort, standardization and appropriate access to a wide range of information critical to achieving Maritime Domain Awareness. The Stakeholder Board co-chairs will develop a charter within 60 days of the appointment of a Director of GMSA Enterprise.

The Stakeholder Board's efforts will focus on optimizing and guiding information sharing and the development of capabilities related to the key functional aspects of Maritime Domain Awareness; collection, fusion, analysis and dissemination of data, information, and intelligence. At a minimum, the board will convene quarterly to:

- Provide the MSPCC and national security leaders, through the co-chairs, recommendations to update strategic-level guidance and revise policy as appropriate; particularly policies and standards to promote information and intelligence sharing across a wide range of domestic and international maritime stakeholders;
- Identify statutory, policy, legislative and cultural issues impeding the integration of information and intelligence and efforts to achieve MDA;
- Discuss activity of and provide guidance to the GMII and GMSA Enterprises to improve the availability and integration of maritime data, information and products;
- Foster an environment that facilitates intelligence and information sharing and unity of effort within the GMCOI through leadership, policy development, oversight and accountability;
- Coordinate implementation of multi-agency tasking and requirements related to maritime intelligence and information sharing;
- Develop a process, and provide a venue for the resolution of cross-jurisdictional issues, including intelligence and information sharing disputes;
- Ensure subsequent follow-on versions of this CONOPS, and the Integrated Investment Strategy address the equities of both the GMII and GMSA Enterprise and include evaluation based on most recent maritime threat assessment;
- Ensure Global Maritime Domain Awareness information architecture and products support the requirements of federal, state, local, tribal, private sector, and international stakeholders at all levels worldwide;
- Facilitate integration and prioritization of requirements and resources for Global Maritime Domain Awareness; and
- Assist in prioritizing goals and objectives for GMSA that are consistent with interagency priorities.

8.3 *Global Maritime Community of Interest Intelligence Enterprise*

National Security Presidential Directive-41/Homeland Security Presidential Directive-13 underscores the importance of securing the Maritime Domain. The Global Maritime Intelligence Integration Plan is one of the eight supporting plans to the National Strategy for Maritime

Security. The GMII Plan defined the GMII Enterprise Director's roles and responsibilities in using existing capabilities to integrate all available intelligence regarding potential threats to U.S. interests in the Maritime Domain.

Nothing in the MDA CONOPS either changes or restricts the authorities and responsibilities assigned by the GMII Plan to the Director of GMII Enterprise and staff.

8.4 *Director Global Maritime Situational Awareness Enterprise*

The Director GMSA Enterprise is responsible for effective access to maritime information and data critical to building the situational awareness component of Global MDA. The Director will develop and recommend policy guidance for coordinated collection, fusion, analysis and dissemination of GMSA information and products, as well as information integration policies, protocols and standards across the GMSA Enterprise that are consistent with those established under GMII Enterprise. The Director will also recommend improvements to situational awareness-related activities supporting maritime information collection, fusion, analysis and dissemination. The Director GMSA Enterprise will be a career senior executive or flag officer designated by mutual agreement between the Secretary of Defense and Secretary of Homeland Security. The Director will co-chair the MDA Stakeholder Board and be a member of the MSPCC. The Director and staff should collectively have the background and experience to represent federal, state, local, tribal, private sector and international maritime stakeholders who are not part of the Intelligence Community. The Director and staff will be supported by a GMSA Cabinet level organization.

A GMSA Cabinet-level organization will provide administrative support to the Director, GMSA Enterprise and staff. This will include identification of office space, associated administrative supplies and basic services. The Cabinet level organization will act as advocate and sponsor for GMSA findings and recommendations that require federal level attention such as appropriate legislative changes proposals. Interagency policy recommendations will be processed through the MDA Stakeholder Board to the Maritime Security Policy Coordinating Committee. Designation as the Cabinet level organization does not bring with it any additional authorities. The authorities necessary to achieve MDA are a result of the cumulative authorities of the agencies that make up the GMSA Enterprise.

The Department of Homeland Security will be the initial Cabinet-level host organization for the GMSA Enterprise and shall ensure the enterprise is established upon approval of this Concept of Operations.

The GMSA staff will consist of and be supported by dedicated subject matter experts from across the federal government as selected by the Director from departmental nominees – preferably on full-time two to three year detail assignments, consistent with agency funding and mission. At a minimum, nominees should come from the Department of Homeland Security, Department of Defense, Director of National Intelligence, Department of Justice, Department of Transportation, Department of Commerce, Department of State, Department of the Treasury, and Department of Energy's National Nuclear Security Administration. Specifically, Customs and Border Protection, Federal Bureau of Investigation, Immigration and Customs Enforcement, the Intelligence Community, US Coast Guard, US Navy and the Maritime Administration should provide full-time representatives to the GMSA staff based on articulated needs and skill sets from the Director of GMSA. Additionally, the need to understand the vast and complex

mechanisms of financial transactions that underpin the maritime environment dictate that subject matter expertise in these areas be accessible to or resident with the GMSA Director and staff. Until otherwise determined, the director and staff will be located at a single facility, in the Capital Area Region, easily accessible by all members of the maritime community of interest that may include representation from additional law enforcement agencies, commercial maritime and related industries. Within one year, and annually thereafter, the Director of GMSA will provide the MDA Stakeholder Board with a review of GMSA staffing validating or recommending changes to the mix of staff positions. The GMSA staff will be initially organized to address:

- domestic information;
- international information;
- private Sector information;
- information systems and technology to include initiative such as MDA Data Sharing Community of Interest (DS COI); and
- Enterprise Hub coordination.

It is envisioned that, as technical capabilities increase over time, coordination will become primarily virtual, with MDA users networked by a multi-level security and access, services-oriented architecture which may supersede this staffing requirement. However, in the near term success will be contingent upon co-location of lead agency representatives with a primary focus on improving information sharing.

The GMSA Director and staff will not have direct operational responsibilities. However, along with responsibility for enhancing information sharing within the GMCOI, the GMSA Director will be an advocate for organizations that collect, fuse, analyze, disseminate, archive and maintain maritime-related information. The GMSA Director and staff will:

- identify and disseminate specific standards and protocols for information exchange and access in the Global Maritime Community of Interest shared information space. This includes the identification and inclusion of new or existing maritime data sources for the shared information space;
- provide guidance and oversight to the GMSA Enterprise to improve the availability and integration of maritime data, information and products;
- conduct community-wide assessments of capabilities that support GMSA to ensure alignment of customer requirements with community information access processes, and relationships between entities within the GMSA community of interest;
- monitor implementation of MDA initiatives including the Integrated Interagency Investment Strategy and provide an annual report to the MDA Stakeholder Board;
- monitor MDA effectiveness. Develop and execute an assessment plan to include an exercise program and performance measures, and provide an annual report to the MDA Stakeholder Board;
- engage the GMCOI, to gain federal, state, local, tribal, international, and private sector participation;

- coordinate and align efforts with the GMII Enterprise;
- coordinate community-wide inputs in developing future spirals of this CONOPS and the Integrated Interagency Investment Strategy. Solicit input from appropriate maritime stakeholders and ensure consistency with GMII Enterprise;
- work with the Enterprise Hubs to develop and implement a MDA Services Oriented Architecture;
- advocate policy modifications to overcome impediments to achieving MDA;
- develop and disseminate information sharing lessons learned;
- develop and recommend policies and procedures that integrate financial transaction information with MDA pillar activities;
- work in conjunction with the GMII Enterprise Director to minimize information access impediments and ensure information exposed to the GMCOI is disseminated at the lowest appropriate security level;
- recommend policy and processes to ensure data integrity and data security;
- serve as the advocate for information sharing practices recommended by Enterprise Hubs, ensuring all possible data relating to the MDA pillars and finance are available to the end users;
- assist in the resolution of cross-jurisdictional issues, including intelligence and information sharing disputes between stakeholders;
- recommend policy regarding access to GMSA information by international, commercial, or other entities;
- interface with members of the GMCOI to determine priorities and ensure priorities are appropriately focused; and
- facilitate closer cooperation with international, state, regional, local and tribal officials and organizations, consistent with the International Outreach and Coordination Strategy of the National Strategy for Maritime Security.

9. Interagency Coordination

MDA must leverage resources and expertise held throughout the GMCOI to improve our ability to detect, prevent and apprehend terrorists and criminals. To maximize intelligence and information sharing, all members of the GMCOI must share information and intelligence, communicate, collaborate, and coordinate their efforts to the maximum extent possible. Effective MDA relies on a network architecture that links maritime intelligence and information providers with all MDA users, decision makers and operational commanders. The desired state is a global, web-enabled, net-centric enterprise; a fully networked and virtually coordinated MDA picture. The network will have a multi-level security and access structure, as appropriate, tailored to enable users to pull appropriate information and data, and to receive alerts and warnings pushed from the network to users.

Non-material solutions will play a significant role in achieving MDA. New doctrine, organizations, and training programs, along with new ways of using people and facilities will

play an important role in engaging and integrating all members and aspects of the GMCOI. Although this document is intended to address concepts and not solutions this approach is worthy of mention. Capability gaps will be addressed in the MDA investment strategy while potential solutions will be developed and evaluated through follow-on efforts.

Current technical, cultural, political, and policy limitations inhibit day-to-day attainment of MDA. In the next subsection, this CONOPS proposes the establishment of Enterprise Hubs based on the pillars of MDA. They will be located at existing agency analysis centers with representation from other members of the GMCOI as needed. These Hubs will be the lead coordinators for their MDA pillar and facilitate sharing information and intelligence among the GMCOI.

9.1 *Enterprise Hubs*

Enterprise Hubs will be developed from within existing organizations with capabilities that already make substantial contributions to MDA in one or more of the following subject areas:

- vessels;
- cargo;
- people;
- infrastructure; and
- architecture management.

Designation as an Enterprise Hub confers two primary responsibilities; overall coordination of information flow for the respective subject area both domestically and internationally, and facilitating the sharing of related intelligence, information, and data. Enterprise Hubs are intended to leverage their experience and expertise to provide leadership for the community in a particular area, not to be the exclusive federal provider of information and products for that subject area. The near-term concept calls for MDA Enterprise Hubs for the four MDA pillars, as well as architecture. Agencies will require additional personnel, resources, and interagency representation to fulfill liaison and subject matter expert functions.

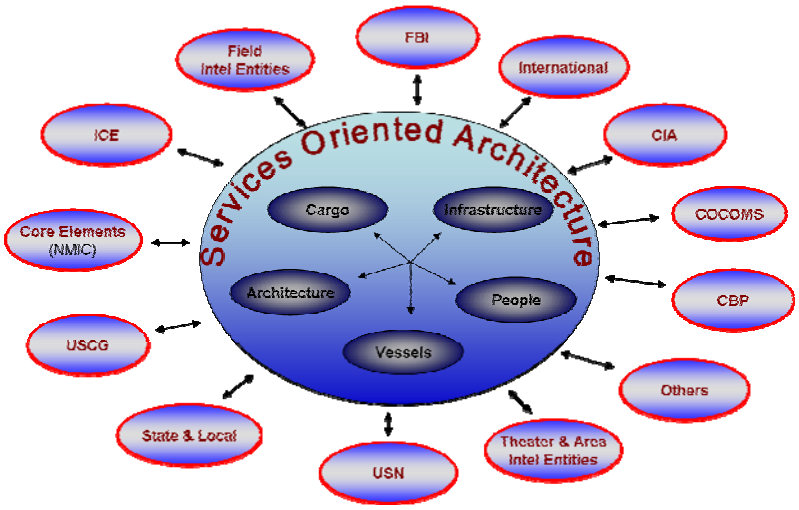
These Enterprise Hubs need to be linked to intelligence and information providers and be able to share pertinent data with the GMCOI. Each Enterprise Hub will receive intelligence, information, and warnings generated by the GMII and GMSA communities, and each Hub will make available GMSA data and information to appropriate decision-makers and GMI partners. Current political, cultural and fiscal limitations to the implementation of viable technologies dictate a regional or local approach to analysis, fusion, and dissemination. In the near-term, the analysis and fusion of intelligence and information regarding the MDA pillars will be performed by those local, regional, and national entities that currently perform an analysis function. Although a department or agency may be designated an Enterprise Hub lead, this designation, in and of itself, does not give it an analysis function. However, that same department or agency may, as part of its mission set, possess an analytical capability. In the future, coordination will be largely virtual, with all MDA users networked by a multi-level security, services-oriented architecture. There may also be a need for additional Hubs in the future to address areas such as finance, ownership, and international and regional issues.

While agencies that host Enterprise Hubs perform collection, fusion and analysis consistent with their current roles and responsibilities, these functions compliment the primary objective of a Hub. The Enterprise Hubs are sources of subject matter expertise for the GMSA and GMII Enterprises, administered by the GMSA Director.

9.1.1 Functions

MDA Enterprise Hubs will:

- lead interagency information coordination for their respective pillar of MDA information;
- facilitate the sharing of intelligence, information and data;
- inventory and catalog the databases and information sources that contribute to achieving MDA, serve end user requirements and ensure availability for access via the web enabled architecture;
- develop a system to track and assess new and proposed initiatives associated with the maritime domain (it is incumbent upon each agency to inform the respective Hub of new programs and initiatives);
- maintain a directory of world-wide MDA-related capabilities, procedures, and ongoing activities for their respective MDA pillar;
- establish a process or protocol for communicating MDA-related needs, developments, and information to federal, state, local, tribal, private sector, and international stakeholders;
- coordinate interagency development of capability goals corresponding to levels of awareness in Appendix D;
- identify issues that inhibit achieving MDA;
- advocate near-term improvements to information sharing that enhance fusion and analysis of maritime data by stakeholder agencies as the enterprise moves toward a SOA;
- maintain consistent liaison with other Enterprise Hubs, establish a formal quarterly summit to exchange needs, ideas, developments and standards;
- facilitate progress toward a net-centric architecture within their respective MDA pillar; and
- address the following areas and provide recommendations to the governing organization for common standards of
    - collection,
    - fusion/analysis,
    - dissemination,
    - archive/maintenance,
    - metrics,
    - data integrity, and
    - data security.



MDA Enterprise Hubs

9.1.2 MDA Architecture Management

Due to the unique characteristics and subject matter expertise required of the net-centric MDA architecture, designation of a lead federal agency (LFA) to address architecture development, management, and maintenance is required. This agency will function in a similar manner to the Enterprise Hubs and will be charged with the management and migration of these Hubs to a virtual environment. The LFA will serve as the MDA Director's subject matter expert for all network management and maintenance considerations and will address the following requirements:

- define architecture compatibility standards;
- host or identify those who will host, net-centric enterprise services;
- recommend associated technology investments;
- enable the Service Oriented Architecture functionality;
- manage network security and appropriate information assurance measures; and
- maintain registries and provide identification, discovery, and access services.

9.1.3 Lead Agencies and Rationales

Enterprise Hubs are responsible for ensuring that the functions listed in paragraph 9.1.1 are accomplished for their respective area of expertise world-wide even if the Enterprise Hub lead has an operational focus in a particular geographic area. Additionally, each Enterprise Hub will coordinate its activities with the other Enterprise Hubs to ensure unity of effort. Other agencies may take the lead for various sub-components of the Enterprise Hub responsibilities (either certain geographic areas or individual functions) but the overall responsibility for leading the Enterprise Hub's activities rests with the designated lead agency. The recommendations for lead agencies and the supporting rationale are:

- Vessel—DoD-DHS/Office of Naval Intelligence–USCG Intelligence Coordination Center (ONI-ICC)—The Vessel Tracking Hub supports the MDA effort of the United States Government and those international and domestic organizations that are recognized partners in the MDA effort. There are numerous ongoing international, regional and national efforts to develop vessel information systems that include vessel tracking. Additionally, there are a number of private companies that offer similar services. Information from these external initiatives may be imported and utilized by the Vessel Enterprise, but the Vessel Enterprise Hub plays no official role in the development, management or governance of these external MDA systems. As the recommended Enterprise Hub for Vessels, the ONI/ICC will fulfill the functions listed in paragraph 11.1.1. Examples of functions to be performed by the Vessel Hub are provided in Appendix E.

  DoD-DHS/ONI-ICC will lead the Vessel Hub because of the existing expertise in all-source analysis of vessel related information and intelligence. Furthermore, the MDA Plan designates the National Maritime Intelligence Center (NMIC) as the central point of connectivity to fuse, analyze, and disseminate information and intelligence for shared awareness across classification boundaries.[11] As the capabilities of the MDA community of interest mature, the suitability and necessity of the NMIC as the Enterprise Hub for Vessels will be reevaluated;

- Cargo—DHS/CBP—As the recommended Enterprise Hub for Cargo, CBP will fulfill the functions listed in paragraph 11.1.1.

  CBP will lead the Cargo Hub because it is the federal agency responsible for admissibility decisions regarding all international cargo. CBP uses high-level analysis tools and access to extensive data sets in order to identify and respond to threats within the supply chain. CBP also operates the 24 x 7 National Targeting Center, which is a nationally recognized analytical and tactical targeting facility. CBP familiarity with the maritime supply chain makes them suited for leading the Cargo Enterprise Hub. The Cargo Enterprise Hub will require close cooperation between CBP and ONI who have complementary missions within this MDA pillar. Examples of functions to be performed by the Cargo Hub are provided in Appendix E;

- People—DHS/CBP—As the recommended Enterprise Hub for People, CBP will fulfill the functions listed in paragraph 11.1.1.

  CBP will lead the People Hub because it is the federal agency responsible for admissibility decisions regarding all international travelers. As with cargo, CBP uses high-level analysis tools and access to extensive data sets in order to identify and respond to threats from among passengers and crewmembers arriving in the US. CBP also operates the 24X7 National Targeting Center, which is a nationally recognized analytical and tactical targeting facility. CBP familiarity with the marine transportation system makes them suited for leading the People Enterprise Hub. Examples of functions to be performed by the People Hub are provided in Appendix E;

---

[11] *National Plan to Achieve MDA*, p. ii.

- Infrastructure—DHS/Office of Infrastructure Protection (OIP)/National Infrastructure Coordinating Center (NICC)—As the recommended Enterprise Hub for Infrastructure, OIP/NICC will fulfill the functions listed in paragraph 11.1.1.

  OIP/NICC will lead the Infrastructure Hub. As the operational arm of OIP and a core component of the National Operations Center (NOC), the NICC monitors the status of the Nation's critical infrastructure and key resources (CI/KR) on an ongoing basis. During an incident, the NICC provides a mechanism and process for information sharing across the CI/KR sectors through appropriate information-sharing entities such as the Sector Coordinating Councils, Government Coordinating Councils, and Information Sharing & Analysis Centers. To foster information sharing and coordination, private sector representatives may provide information to the NICC. While NICC's focus is on US infrastructure, NICC experience is applicable world-wide. Examples of functions to be performed by the Infrastructure Hub are provided in Appendix C; and

- Architecture—DoD/Department of the Navy (DON)—As the recommended Enterprise Hub for Architecture Management, DON will pursue development of an information architecture as described in section 9.

  DON will lead the Architecture Management Hub as it has a central operational authority for space, information technology requirements, networks and information operations. This organization is responsible for operation of a secure and interoperable network that will enable effects-based operations and innovation; to coordinate and assess operational requirements for and use of network/command and control/information technology/information operations and space. While this is DON focused, the concepts have immediate applicability to MDA across the GMCOI.

9.1.4 Enterprise Hub Example

Due to an agency's difficulty in obtaining passenger and crew information, CBP, as the People Enterprise Hub, calls a meeting of all GMCOI agencies with an interest in people in the Maritime domain. The intent of this meeting is to identify any impediments to the exchange of information on people as it pertains to improving MDA. CBP hosts the meeting at their facility, sets an agenda, ensures a wide distribution of the meeting notice to engage the full GMCOI, facilitates discussion, takes and posts meeting notes, and provides a full report on the results of the meeting to the MDA governance entity and other Enterprise Hubs. As a follow-up, CBP tracks action items resulting from the meeting, hosts follow-up meetings as necessary, ensures relevant documents are posted to the Enterprise Hub web site, and continues to update the MDA governance entity on progress. In the event that the MDA governance entity has an inquiry related to legal or other issues limiting the exchange of people information, they would reach out to that Hub. CBP would coordinate development of a response and provide that information to the MDA governance entity.

10. Assessment

A critical component of achieving and enhancing MDA is the development of a means to assess progress toward MDA objectives. This and each subsequent iteration of the National MDA CONOPS will generate a spiral of the National MDA Investment Strategy that prioritizes gaps in our ability to achieve MDA. The governing organization will lead a periodic review, assessment

and evaluation of progress toward closing the capability gaps delineated in Investment Strategy spirals. This evaluation will be provided to the Maritime Policy Coordinating Committee at least biennially to ensure that efforts and expenditures applied toward MDA objectives are effectively sequenced and synchronized.

10.1 *Spiral Development*

This CONOPS is the first in a series of spirals. This spiral, which describes the federal mechanism for coordinating the exchange of MDA-related information and intelligence, will be supplemented by editions that more thoroughly elaborate on intra-departmental processes, international and commercial entity involvement, and the roles of state, local and tribal maritime stakeholders. These follow-on spirals will seek to encourage a rapid increase in the sharing of maritime information within and between regions. The resultant transparency will enhance our global maritime awareness and mitigate the effects of transnational dangers presented by natural disasters, pandemic diseases, human trafficking, and criminal organizations. Properly developed, a network of international maritime partnerships will bring security at sea and an enhanced velocity of safe commerce around the globe.

This and each CONOPS spiral must be assessed against a broad range of threats to our national security in order to determine gaps in our ability to achieve MDA. While it is impossible to predict all possibilities, analyzing each CONOPS spiral through experimentation, gaming, modeling, simulation, and exercises will determine existing MDA capabilities and agency requirements to perform their respective missions.

10.2 *Investment Strategy*

The investment strategy will align means to objectives and establish the relative importance of identified shortfalls in our ability to achieve MDA. Upon determination of existing capabilities and agency requirements through operational analysis, identified capability gaps will need to be prioritized using the most recent National Intelligence Estimate. Upon approval, lead and supporting departments within the U.S. Government will determine the optimal method for addressing the capability gap.

11. Conclusion

The United States faces a complex and dynamic security environment and is engaged in a Global War on Terror with stateless actors. Natural disasters, traditional state threats and emerging challenges from within our borders also threaten our security. These challenges to our security and economic prosperity require a new mindset—one that takes a comprehensive view of all risks, vulnerabilities, threats, consequences and opportunities, and enables response through an active, layered defense-in-depth.

The criticality of the maritime domain to international trade and economic prosperity makes it a likely target for exploitation by terrorists. To achieve an active, layered defense and improve operational efficiencies, the Nation must harness or develop the means to achieve a more comprehensive and effective understanding of the maritime domain.

MDA is the effective understanding of anything associated with the global maritime domain that could impact the security, safety, economy, or environment of the United States. MDA is

important not only for its role in Homeland Security and protecting U.S. territory, people, and infrastructure, but is equally important in its ability to promote U.S. National interests abroad. MDA will enable operational forces to stem the flow of illegal cargoes around the world, limit the spread of Weapons of Mass Destruction, and interdict terrorists well before they approach the territory of the United States and its allies.

Effective intelligence and information sharing is critical to understanding the maritime domain and improving safety and security of the United States. For information sharing to succeed, there must be trust—the trust of information providers, the users of information, policymakers, and most importantly of the public. Each of these must believe that information is being shared appropriately, consistent with law and in a manner protective of privacy and civil liberties.

MDA requires the coordinated focus and unity of effort across a broad range of federal, state, local, tribal, private sector and international partners. The MDA governance structure must provide sufficient direction in developing policy and standards to guide individual agencies and partners in sharing information and intelligence and working together to ensure continued alignment of efforts to achieve MDA.

An MDA architecture founded upon net-centric principles will provide a secure, collaborative, information-sharing environment and unprecedented access to decision-quality information. A fundamental attribute of the net-centricity is the ability for any consumer of information to get the information that is needed, when it is needed. The concept of a UDOP is founded upon net-centricity.

This document proposes the designation of Enterprise Hubs as an interim step between today's relatively restricted approach to information and intelligence sharing and the desired net-centric architecture that will enable an extended sharing environment. The two primary responsibilities of the Enterprise Hubs are coordination of information flow for the respective subject area both domestically and internationally, and facilitating the sharing of related intelligence, information, and data within and across Hubs and throughout the maritime community of interest. In the future these Hubs will grow into a virtual analysis and fusion network as technology capabilities mature.

Ultimately the desired state does not specify a requirement to know all things about all activities in the maritime domain, but rather for the ability to gain in-depth information on any event when it is needed. Existing resources, technologies, legal prohibitions, and policies limit the ability of maritime stakeholders to persistently monitor the maritime domain. Concepts such as parsing the maritime domain and levels of awareness will provide a means for prioritizing the types of information needed and areas of the world where information must be collected.

This *National Plan to Achieve Maritime Domain Awareness* sets forth the path toward achieving understanding of the maritime domain. The MDA CONOPS is an overarching document applicable to all federal agencies under which individual departments and agencies can develop specific operational guidance, tactics, techniques and procedures. The implementation of this document will be continuous. Follow-on iterations will address intelligence and information sharing with state, local, tribal, private sector and international stakeholders. Achieving the desired capabilities call for continued investment of our Nation's intellectual, technological, human and financial resources, as well as a partnership with other nations.

Nothing in this plan impairs or otherwise affects the authority of the Secretary of Defense over the Department of Defense, including the chain of command for military forces from the President and Commander in Chief, to the Secretary of Defense, the command of military forces, or military command and control procedures.

Appendix A—Maritime Security Lexicon

This lexicon has been developed to aid in understanding MDA-related terms found in the CONOPS and other MDA documents. It will be edited as required in the future to support clarity. The lexicon is broken into two parts: acronyms and glossary.

Appendix A—MDA Acronyms

Acronym	Meaning
ACSD	Advanced Container Security Device
AES	Automated Export System
AIS	Automatic Identification System
AMOC	CBP Air and Marine Operations Center
AMS	Automated Manifest System
ANOA	Advanced Notice of Arrival
AOI	Area of Interest
AOR	Area of Responsibility
APIS	Advance Passenger Information System
ATS	Automated Targeting System
BFT	Blue Force Tracking
C2	Command and Control
CBP	Customs and Border Protection
CBRNE	Chemical, Biological, Radiological, Nuclear, and High-Yield Explosive
CDC	Certain Dangerous Cargo
CGDN+	Coast Guard Data Network Plus
CIA	Central Intelligence Agency
CIP	Common Intelligence Picture
CI/KR	Critical Infrastructure & Key Resources
CMAN	Coastal Marine Automated Network
COE	Common Operating Environment
COI	Contact of Interest
COI	Community of Interest

CONOPS	Concept of Operations
COP	Common Operational Picture
COTP	Captain of the Port
CSI	Container Security Initiative
C-TPAT	Customs-Trade Partnership Against Terrorism
DADS	Deployable Autonomous Distributed System
DCGS	Distributed Common Ground/Surface System
DCS	Defense Communications System
DO	Domestic Outreach Plan
DOE	Department of Energy
DON	Department of Navy
DOD	Department of Defense
DOT	Department of Transportation
DDN	Defense Data Network
EEZ	Exclusive Economic Zone
ENOA	Electronic Notice of Arrival
EOC	Emergency Operations Center
EPIC	El Paso Intelligence Center
GCCS	Global Command and Control System
GIG	DoD's Global Information Grid
GIS	Geospatial Information Systems
GMCOI	Global Maritime Community of Interest
GMI	Global Maritime Intelligence
GMII	Global Maritime Intelligence Integration
GMSA	Global Maritime Situational Awareness
GPS	Global Positioning System
GWOT	Global War On Terror
HAZMAT	Hazardous Materials
HIV	High Interest Vessel
HD	Homeland Defense
HS	Homeland Security

HSC	Homeland Security Council
HSIN	Homeland Security Information Network
HSOC	Homeland Security Operations Center (currently National Operations Center)
HSPD	Homeland Security Presidential Directive
IC	Intelligence Community
ICC	USCG Intelligence Coordination Center
ICE	Immigration and Customs Enforcement
IMO	International Maritime Organization
INMARSAT	International Marine/Maritime Satellite (Communications)
INT	Intelligence
IRVMC	Inland River Vessel Movement Center
ISPS	International Ship and Port Facility Security
IO	International Outreach and Coordination Strategy
IT	Information Technology
IT	Implementation Team
ITDS	International Trade Data System
JFMCC	Joint Force Maritime Component Commander
JHOC	Joint Harbor Operations Center
JIATF	Joint Interagency Task Force
JIC	Joint Intelligence Center
JIOC	Joint Intelligence Operations Center or Joint Information Operations Center
JTTF	Joint Terrorism Task Force
KM	Knowledge Management
LFA	Lead Federal Agency
LRIT	Long Range Identification and Tracking
M/V	Motor Vessel
MARSEC	Maritime Security Level
MATTS	Marine Asset Tag and Tracking System
MCI	Maritime Critical Infrastructure
MDA	Maritime Domain Awareness

MDZ	Maritime Defense Zone
MHQ	Maritime Headquarters
MIFC	USCG Maritime Intelligence Fusion Center
MIO	Maritime Interception Operations
MIRP	Maritime Infrastructure Recover Plan
MOC	Maritime Operations Center (USN)
MOTR	Maritime Operational Threat Response
MPA	Maritime Patrol Aircraft
MSPCC	Maritime Security Policy Coordinating Committee
MSWG	Maritime Security Working Group
MTS	Marine Transportation System
MTSA	Maritime Transportation Security Act
MTSS	Maritime Transportation System Security Recommendations
NCPC	National Counter Proliferation Center
NCTC	National Counterterrorism Center
NICC	National Infrastructure Coordination Center (DHS)
NM-COP	National Maritime – Common Operating Picture
NMIC	National Maritime Intelligence Center (ONI and ICC combined)
NMSAC	National Maritime Security Advisory Committee
NMSP	National Maritime Security Plan
NNSA	National Nuclear Security Administration
NOA	Notice of Arrival
NOC	National Operations Center (formerly HSOC - Homeland Security Operations Center)
NPAMDA	National Plan to Achieve Maritime Domain Awareness
NPRN	National Port Readiness Program
NSMS	National Strategy for Maritime Security
NSPD	National Security Presidential Directive
NTC	CBP National Targeting Center
NVMC	National Vessel Movement Center
OIP	Office of Infrastructure Protection

ONI	Office of Naval Intelligence
PAWSS	Ports and Waterways Safety System
PBRS	Pleasure Boat Reporting System
RMSI	Regional Maritime Security Initiative
SA	Situational Awareness
SANS	Ship Arrival Notification System
SCC	Sector Command Center (USCG)
SCC-J	Sector Command Center-Joint (USCG/USN)
SIV	Special Interest Vessel
SLOC	Sea Lines of Communication
SOA	Service Oriented Architecture
SOLAS	International Convention for the Safety of Life at Sea, 1974
SPOE/SPOD	Seaport of Embarkation/Seaport of Debarkation
TIDE	Terrorist Identity Datamart Environment
TSDB	Terrorist Screening Data Base
TSOC	Transportation Security Operational Center
UDOP	User Defined Operational Picture
USCG	United States Coast Guard
VIS	Vessel Identification System
VISA	Voluntary Intermodal Sealift Agreement
VMS	Vessel Monitoring System
VOI	Vessel of Interest
VTS	Vessel Traffic System/Service
WMD	Weapons of Mass Destruction

Appendix A—MDA Glossary

TERM	DEFINITION
Advanced Container Security Device (ACSD)	ACSD will provide the next generation of maritime shipping container security devices with multiple sensing modalities, "smart" condition monitoring, automated alerting, and advanced communications, by focusing on those technologies that are not yet ready for commercial applications. ACSD is the linchpin for enabling expanded container security sensing and alerting technologies to be incorporated into the global supply chain.
Anomaly Detection	Detecting threats by looking for activity that is different from normal behavior.
Architecture	A framework or structure that portrays relationships among all elements of a subject force, system, or activity.
Area of Responsibility (AOR)	The geographical area associated with a command within which the commander has the authority to plan and conduct operations.
Automatic Identification System (AIS)	AIS is a reporting system mandated by IMO for vessels 300 gross tons and above. Currently the system provides positional and identification information via a VHF transceiver system. The system has the ability to transmit information via various communications channels. Use of AIS is also required under MTSA of 2002 for commercial vessels operating in navigable waters of the United States that are 65 ft or greater in length and a towing vessel of more than 26 ft in length overall. Additional regulations for AIS use will be added in the future. (See 33CFR, Chapter 1, Part 164).
Break Bulk Cargo	Any commodity that, because of its weight, dimensions or incompatibility with other cargo is shipped outside of standard containers.
Bulk Cargo	That which is generally shipped in volume where the transportation conveyance is the only external container; such as liquids, ore, or grain.
Command and Control (C2)	The exercise of authority and direction by a properly designated commander over assigned and attached forces in the accomplishment of the mission. C2 functions are performed through an arrangement of personnel, equipment, communications, facilities, and procedures employed by a commander in planning, directing, coordinating, and controlling forces and operations in the accomplishment of the mission. (JP 1-02)
Commercial Vessel	A vessel (i.e. boat, tugboat, barge or ship) engaged in commercial trade or that carries passengers for hire. This would exclude pleasure craft or warships.

Common Intelligence Picture (CIP)	The CIP is a compendium of relevant intelligence information shared by more than one command. It is fed by a wide variety of intelligence sensors, databases and current analysis. The CIP will focus on identifying threats to the maritime domain, providing insight into threat capabilities and intent. CIP products may be tailored to meet the requirements of operational and tactical commanders and strategic decision makers. The CIP facilitates collaborative analysis and permits rapid insertion of relevant intelligence into the COP, enhancing situational awareness at every echelon.
Common Operational Picture (COP)	A display of relevant information shared by more than one command. The COP provides a shared display of friendly, enemy/suspect, and neutral tracks on a map with applicable geographically referenced overlays and data enhancements. The COP environment may include distributed data processing, data exchange, collaboration tools, and communications capabilities. The COP may include information relevant to the tactical and strategic level of command. This includes, but is not limited to, geographic information systems data, assets, activities and elements, planning data, readiness data, intelligence, reconnaissance and surveillance data, imagery, and environmental data.
Concept of Operations (CONOPs)	A CONOPs is a description of how discrete, collective, or combined capabilities will be managed and employed to achieve desired objectives, or to test experimental technologies or concepts. It can inform operators and planners as well as resource and acquisition sponsors, other departments and branches of government, industry, and the media. It is categorized by purpose, scope, level of integration, and temporal frame of reference. A CONOPs can address issues pertaining to manning, equipping, training, maintenance, and administration. A CONOPs takes the CONCEPT and adds the who, where, when, and perhaps most importantly <u>how</u>. A CONOPS is a proposal that requires validation.
Consequence	An assessment of the impact in the aftermath of a conducted threat against a vulnerability(ies).
Critical Asset	A specific entity that is of such extraordinary importance that its incapacitation or destruction would have a very serious, debilitating effect on the ability of a nation to continue to function effectively.
Critical Infrastructure	Systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters.

Detect	Detection is an event during surveillance that is dependent upon the capability of sensors and/or intelligence and the characteristics of the targets. Specific intelligence may direct sensors to concentrate in an area to detect a particular Target of Interest (TOI).
Fusion	1. Combining of automatically correlated information with the data that refines the information or presents it in intuitive format. Fused data in many cases will arrive later than real or near-real time data. 2. In intelligence usage, the process of examining all sources of intelligence and information to derive a complete assessment of an activity. 3. Combining disparate data elements which apply to the same object or activity to create a more complete picture.
Fusion Center	A physical location to accomplish fusion. Normally has a sufficient automated processing capability to assist in the process.
Global Maritime Community of Interest (GMCOI)	Includes, among other interests, the federal, state, and local departments and agencies with responsibilities in the maritime domain. Because certain risks and interests are common to government, business, and citizen alike, community membership also includes public, private and commercial stakeholders, as well as foreign governments and international stakeholders.
High Interest Vessel (HIV)	A vessel intending to enter a U.S. port that may pose a high relative security risk to the port.
Infrastructure	Refers to the Marine Transportation System (MTS) and those facilities, structures, and assets vital to U.S. and global interests, such as roads, buildings, dams, locks, utilities. (modified definition, see MIRP pg8 sixth bullet).
Intelligence	1. The product resulting from the collection, processing, integration, analysis, evaluation, and interpretation of available information concerning foreign countries or areas. 2. Information and knowledge about an adversary obtained through observation, investigation, analysis, or understanding.
Joint Force Maritime Component Commander (JFMCC)	The commander within a unified command, subordinate unified command, or joint task force responsible to the establishing commander for making recommendations on the proper employment of assigned, attached, and/or made available for tasking maritime forces and assets; planning and coordinating maritime operations; or accomplishing such operational missions as may be assigned. The joint force maritime component commander is given the authority necessary to accomplish missions and tasks assigned by the establishing commander. Also called JFMCC. (JP 1-02)

Joint Harbor Operations Center (JHOC)	JHOCs are operational command and control facilities staffed by the Navy and Coast Guard, as well as other port centric stakeholders. JHOCs are focused in around a single port and their efforts focus on coordinating operations and information sharing.
Long Range Identification and Tracking (LRIT)	LRIT was established by the IMO Maritime Safety Committee in May 2006 to allow for tracking of vessels greater than 300 gross tons beyond the normal range of AIS. Ships will be required to transmit information including the ship's identity, location and date and time of the position when the mandatory Safety of Life at Sea Convention (SOLAS) amendments come into force. There will be no interface between LRIT and AIS. One of the more important distinctions between LRIT and AIS, apart from the obvious one of range, is that, whereas AIS is a broadcast system, data derived through LRIT will be available only to the recipients who are entitled to receive such information and safeguards concerning the confidentiality of those data have been built into the regulatory provisions. SOLAS Contracting Governments will be entitled to receive information about all commercial ships navigating within a distance 1000 nautical miles off their coast.
Marine Transportation System (MTS)	Consists of waterways, ports and inter-modal connections, vessels, vehicles, and system users, as well as federal maritime navigation systems.
Maritime Critical Infrastructure/Key Assets	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.

Maritime Domain Awareness (MDA)	MDA is the effective understanding of anything associated with the global maritime environment that could impact the security, safety, economy, or environment of the United States. (NSPD-41/HSPD-13, 21 December 2004) The United States must be capable of maintaining a comprehensive knowledge of what is happening within the U.S. Maritime Domain, including visibility of MDA pillars. Only then can it distinguish the myriad of vessels conducting legitimate pursuits from those warranting closer inspection. To gain and effectively use such knowledge, we must collect our own data and fuse that information with data and intelligence from other agencies, analyzing it and disseminating it to support informed decision-making at the strategic, operational, and tactical levels. It is expected that the collection, fusion, analysis, and dissemination will occur at national, regional, and state levels, with further dissemination at the local level. This comprehensive information, intelligence, and knowledge base is termed MDA.
Maritime Headquarters (MHQ)	Navy's primary Command and Control Nodes for generating Maritime Domain Awareness. Navy component commands (NCC), numbered fleets and Navy principal headquarters. Navy principal headquarters are those Navy commands (other than NCCs and Numbered fleets) who have operational responsibilities and report directly to a combatant.
Maritime Operations Center (MOC)	A Navy facility organized, manned and responsible for operational level coordination, synchronization, and guidance of near term planning and execution.

Maritime Security (MARSEC) Level	MARSEC Level: a warning level set for a specified maritime region to reflect the prevailing threat environment to the marine elements of the national transportation system, including ports, vessels, facilities, and critical assets and infrastructure located on or adjacent to waters subject to the jurisdiction of the United States. The concept of MARSEC Levels is contained in the International Ship and Port Facility Security Code for a common understanding by all ships flagged by SOLAS Contracting States and all foreign ports that these ships visit. MARSEC Level 1: a warning level for which minimum appropriate protective security measures shall be maintained at all times. This is the normal operating MARSEC level for the port and is equivalent to YELLOW (Elevated) in the Homeland Security Advisory System. MARSEC Level 2: a warning level for which appropriate additional protective security measures shall be maintained for a period of time as a result of heightened risk of a transportation security incident. This is equivalent to ORANGE (High) in the Homeland Security Advisory System. MARSEC Level 3: a warning level for which further specific protective security measures must be maintained for a limited period of time when a transportation security incident is probable or imminent, although it may not be possible to identify the specific target. This is equivalent to RED (Severe) in the Homeland Security Advisory System.
Monitor	To watch, or keep track of, to the extent necessary to determine the degree of risk.
National Vessel Movement Center (NVMC)	The National Vessel Movement Center (NVMC) is the Coast Guard's centralized facility for processing the Notice of Arrivals for ships entering United States ports. NVMC began operations on 15 October 2001 when the arrival notification requirement was increased from 24 hours to 96 hours. NVMC personnel collect and screen information on the vessel's arrival, cargo and crew/passenger information, information. Vessels, or their agents, provide notification to the NVMC by telephone, internet, e-mail, or fax. Data collected by the NVMC is entered into the Ship Arrival Notification System (SANS) database.
Net-Centric	Exploitation of advancing technology that moves from an application centric to a data-centric paradigm – that is, providing users the ability to access applications and services through Web services – an information environment comprised of interoperable computing and communication components. (Office of the Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer, Net Centric Checklist, 12 May 2004, version 2.1.3)

Net-Centric Environment	A framework for full human and technical connectivity that allows all users and mission partners to share the information they need, when they need it, in a form they can understand and act on with confidence; and protects information from those who should not have it. (Net-Centric Environment Joint Functional Concept, 7 April 2005, version 1.0 – modified for interagency applicability)
Passenger Vessel	Vessels which carry passengers for hire regardless of how classified (i.e., un-inspected passenger vessel, small passenger vessel etc.). For example Cruise Liners, ferries, charter boats, etc., but not privately owned recreational vessels.
Persistent	Constantly repeated, continued, unrelenting, but not necessarily continuous.
Persistently Monitor	The integrated management of a diverse set of collection and processing capabilities, operated to detect and understand the activity of interest with sufficient sensor dwell, revisit rate, and required quality to expeditiously assess adversary actions, predict adversary plans, deny sanctuary to an adversary, and assess results of US/coalition actions. "Persistently monitor" in this Plan refers to an ability to conduct persistent monitoring anywhere on the globe. It is not meant to imply that we can simultaneously do persistent monitoring over the entire globe.
Ports and Waterways Safety System (PAWSS)	The Ports and Waterways Safety System (PAWSS) project provides Vessel Traffic Services (VTS) equipment to facilitate the safe and efficient transit of vessel traffic, prevent collisions, groundings, and environmental damage associated with these accidents. The goal of the PAWSS project is to develop and implement a state-of-the-market, AIS-based VTS with radar, cameras and VHF communications, in selected ports and waterways, using open systems architecture and maximizing commercial off-the-shelf (COTS) technology. Vessel tracking information taken from the PAWSS system can be extracted and reformatted in the Over The Horizon (OTH) Gold message format for use in the Common Operational Environment COP.
Risk	An assessment based on the multiplicative formula Risk equals Vulnerability times Threat times Consequence.
Sector Command Center (SCC)	USCG organization that serves in an operations integration function capacity and is organizationally located to equally support both Response and Prevention Departments with the Sector Command.
Sector Command Center-Joint (SCC-J)	An SCC with USN personnel to augment USCG SCC organization and coordinate operations and planning. SCC-J's are SCC's located in USN Fleet Concentration Areas that incorporate a larger mission set (increased capabilities and responsibilities).

Surveillance	The systematic observation of areas, places, persons, or things, by visual, aural, electronic, photographic, or other means.
Targeting	The process of selecting targets and matching the appropriate response to them taking account of operational requirements and capabilities.
Threat	An assessment based on law enforcement or intelligence reporting of the intent and the capability to engage in a hostile act that exploits a vulnerability(ies).
Track	Tracking is the display or recording of the successive positions of a moving object. Tracking must be maintained to allow decision makers to achieve an end result that is mission and situation specific, including doing nothing, monitoring, interdicting, or eliminating the threat or challenge. Stakeholders, decision makers and operators must provide feedback of tracking quality and success to organization(s) responsible for enhancing MDA to enable improvement in performance.
Track and Database Management	The act of entering, correlating, updating, fusing, de-conflicting, and otherwise maintaining assigned tracks using existing automated tools or manual methods. Each command level has a different track database manager responsible for its associated information responsibilities. (COP Handbook for GCCS 3.02)
Track Correlation	Correlating track information for identification purposes using all available data. (JP 1-02)
Track Management	Defined set of procedures whereby the commander ensures accurate friendly and threat location and disposition, and a dissemination procedure for filtering, combining, and passing that information to higher, adjacent, and subordinate commanders. (JP 1-02)
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 seas lanes to the United States, U.S. maritime approaches, and the high seas surrounding America. (Terms of Reference for PWCS, COMDT COGARD, 231402Z DEC 03)
User Defined Operational Picture	Picture tailored by the individual operator taken from a common source.
Vessel	Every description of watercraft or other artificial contrivance used, or capable of being used, as a means of transportation on water.

Vessel Identification System	Chapter 125 of title 46, U.S. Code, requires establishment of a system to identify all Coast Guard-documented and State-numbered vessels. The system, which is not yet operational, will include information to identify a vessel (e.g., hull identification number, manufacturer, length, hull material, etc.), the vessel owner's name, address, and identifier (e.g., Social Security Number, Taxpayer Identification Number, or birth date and driver license number), and information to assist law enforcement officials. When completed, the system will provide data on nearly 13 million State-numbered vessels, as well as all Coast Guard-documented vessels."
Vessel of Interest	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.
Vulnerability	An assessment of the factual or security weaknesses of a physical object/place or of information.
Weapon of Mass Destruction	Any destructive/explosive device as defined by 18 U.S.C § 921; 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 biological agent, toxin or vector, as defined by 18 U.S.C § 178; or any weapon that is designed to release radiation or radioactivity at a level dangerous to human life. (source: 18 USC 2332a)

Appendix B—List of References

- **MDA Related Reference Documents**
  - **Maritime Security Policy (NSPD-41/HSPD-13)** establishes U.S. policy, guidelines, and implementation actions to enhance global maritime security. It directs that all U.S. Government maritime security programs and initiatives be coordinated in order to achieve a comprehensive and cohesive national effort involving appropriate federal, state, local and private sector entities.
  - **National Strategy for Maritime Security** directs the coordination of United States Government maritime security programs and initiatives to achieve a comprehensive and cohesive national effort involving appropriate Federal, State, local, and private sector entities.
  - **National Plan to Achieve Maritime Domain Awareness** lays the foundation for an effective understanding of anything associated with the Maritime Domain that could impact the security, safety, economy, or environment of the United States and identifying threats as early and as distant from our shores as possible.
  - **Maritime Operational Threat Response** coordinates U.S. Government response to threats against the United States and its interests in the Maritime Domain by establishing roles and responsibilities, which enable the government to respond quickly and decisively.
  - **International Outreach and Coordination Strategy** provides a framework to coordinate all maritime security initiatives undertaken with foreign governments and international organizations, and solicits international support for enhanced maritime security.
  - **Maritime Infrastructure Recovery Plan** recommends procedures and standards for the recovery of the maritime infrastructure following attack or similar disruption.
  - **Maritime Transportation System Security Recommendations** responds to the President's call for recommendations to improve the national and international regulatory framework regarding the maritime domain.
  - **Maritime Commerce Security Plan** establishes a comprehensive plan to secure the maritime supply chain.
  - **Domestic Outreach Plan** engages non-federal input to assist with the development and implementation of maritime security policies resulting from NSPD-41/HSPD-13.
- **MDA Senior Steering Group Documents**
  - **Draft Technology Roadmap Report** summarizes requirements, existing capabilities, and capability gaps focusing primarily on sensor and data fusion technologies.
  - **Draft Common Operational Picture (COP) Report** describes the general attributes and requirements for developing a COP.

- The MDA CONOPS is consistent with and supports the strategic objectives outlined in the following National and Departmental level documents:
  - National Security Strategy;
  - National Strategy for Homeland Security;
  - National Maritime Security Response Plan;
  - National Strategy for Combating Terrorism;
  - The National Defense Strategy of the United States of America;
  - Strategy for Homeland Defense and Civil Support;
  - National Military Strategy; and
  - Maritime Strategy for Homeland Security.
- **Information Sharing Legal Guidance**
  - **U.S. Code—5 USC 552a**—Among the laws most oft cited as restricting sharing information among federal databases is the Privacy Act, which appears in Title 5 U.S. Code section 552a.
  - **U.S. Code—10 USC 371**—Allows information concerning possible criminal activity, collected during the normal course of military training and operations, to be shared with law enforcement.
  - **U.S. Code—10 USC 380**—Provides military personnel authority to brief civilian law enforcement personnel concerning information, technical support, equipment and facilities which are available from DoD.
  - **U.S. Code—13 USC 9**—Protects the confidentiality of information collected by the Census Bureau.
  - **U.S. Code—18 USC 1385**—provides that a court shall enter such orders and take such other action as may be necessary and appropriate to preserve the confidentiality of trade secrets.
  - **U.S. Code—18 USC 1831, 1832, 1905**—Trade secrets currently receive protection by federal law from theft and unauthorized disclosure (18 U.S.C. § 1831 (economic espionage)); (18 U.S.C. § 1832 (theft of trade secrets)); (18 U.S.C. § 1905 (disclosure of trade secrets)). Most states have also adopted the Uniform Trade Secrets Act which provides an additional layer of protection. These protections provide a framework for recovery from losses that may be incurred from unauthorized sharing of confidential information with competitors. Trade secrets may also receive protection when shared with the government.
  - **U.S. Code—26 USC 6103**—Provides limited protection to income tax records.
  - **Foreign Intelligence Surveillance Act (FISA) of 1978**— The Foreign Intelligence Surveillance Act of 1978 (FISA), as amended, established a statutory scheme for the collection of "foreign intelligence" through electronic surveillance and physical search. The scheme allows for court-sanctioned surveillance of a foreign power or an agent of a

foreign power (to include U.S. citizens) within the United States. FISA also permits warrantless surveillance under very limited circumstances.

- **The Homeland Security Act of 2002**—The Homeland Security Act of 2002 is an important legal element in the role of sharing information as it established the Department of Homeland Security (DHS) within the Executive Branch. The DHS was developed to aid in the prevention of and "reduce the vulnerability" of the U.S. to acts of terrorism. While the DHS is not tasked with the power to investigate and prosecute acts of terrorism, the Act requires the Department to monitor coordination between agencies and subdivisions to ensure that even the most tangential piece of information is analyzed to help secure the homeland.
- **USA Patriot Act of 2004, Pub. L. 107-56**— The USA Patriot Act enhances law enforcement techniques and information sharing between executive agencies. This Act removed some barriers to information sharing between law enforcement and intelligence agencies by permitting the disclosure to certain officials of foreign intelligence information gathered as a result of criminal investigation. This information can be disclosed to listed officials for the purpose of aiding a "federal law enforcement, intelligence, protective, immigration, national defense, or national security official in his official duties."
- **The Intelligence Authorization Act of 1997**—The Intelligence Authorization Act of 1997 established a division of the National Security Council (NSC), the Committee on Transnational Threats (CTT), to coordinate U.S. efforts in combating terrorist and other organizations. This group can assist in developing policy and facilitating information sharing between the intelligence community (IC) and law enforcement agencies. Additionally, this Act allows the intelligence community to collect and share information with law enforcement regarding individuals dwelling outside the United States. Information collected can be used for criminal investigation or prosecution purposes through LEGAT, the FBI agent abroad in charge of international elements of a case involving counterintelligence, criminal investigations, and counterterrorism.
- **Intelligence Reform and Terrorism Prevention Act of 2004** (IRTPA)— This Act overhauled the IC, mandating a range of reforms and centralizing in one office key authorities. The Director of National intelligence (DNI) serves as the President's principal advisor and the leader of the IC. Further, the Act made reforms in several important areas of intelligence, including: leadership of the IC; analysis; information sharing; civil liberties; and other areas such as education and training, Federal Bureau of Investigation (FBI) culture, and security clearances. The Act assigns the DNI the responsibility to manage the intelligence budget, ensure coordination and information sharing among the IC agencies, and ensure that the best intelligence is made available to policy makers.
- **National Intelligence Strategy of the United States of America – Transformation through Integration and Innovation, October 2005: The Intelligence Community statement of values, highest priorities and future orientation. Directs through mission and enterprise objectives a plan for action that "our vast intelligence enterprise will become more unified, coordinated, and effective." Through the following tasks, the new approach to "national intelligence" will be a far-reaching reform of previous intelligence practices and arrangements: Integrate the domestic**

and foreign dimensions of U.S. intelligence so that there are no gaps in our understanding of threats to our national security; Bring more depth and accuracy to intelligence analysis; and, ensure that U.S. intelligence resources generate future capabilities as well as present results.

- **The Freedom of Information Act**—The Freedom of Information Act (FOIA) was enacted upon the premise that "the government and the information of the government belongs to the people." FOIA created a "right to know," allowing any person to access federal agency records, provided that such records are not protected under any of nine exemptions. Certain records held by the federal government pertaining to foreign intelligence, counterintelligence or international terrorism are exempted from disclosure by FOIA. Additionally, records specifically authorized under an Executive Order to be kept secret in the interest of national defense are exempted from disclosure.
- **U.S. SAFE WEB Act**—The U.S. SAFE WEB Act provisions help to protect consumers from international fraud and deception. The key provisions are:
  - broadening reciprocal information sharing - allows the FTC to share confidential information in its files in consumer protection matters with foreign law enforcement officials, subject to appropriate confidentiality assurances;
  - expanding investigative cooperation - allows the FTC to conduct investigations and discovery to help foreign law enforcers in appropriate cases; and
  - obtaining more information from foreign sources - protects information provided by foreign enforcers from public disclosure if confidentiality is a condition of providing it.
- **"Deemed export laws"**—Laws restrict sharing information with foreign nationals. Laws that limit whether foreign nationals working or studying at U.S. universities may be exposed to secret or sophisticated technology, otherwise referred to as "deemed exports." Whatever net-centric architecture we develop must consider these laws when developing the access & security protocols.
- **Communications Assistance for Law Enforcement Act (CALEA) of 1994**—addresses telecommunications carriers' assistance to law enforcement in executing electronic surveillance pursuant to court order or other lawful authorization.

- **Information Sharing regulations**
  - **19 CFR 4.7**—This regulation requires that vessel masters carrying U.S.-bound containerized cargo and non-exempt break-bulk cargo must submit an electronic cargo declaration to CBP 24-hours in advance of lading the cargo onboard the vessel at the foreign seaport.
  - **19 CFR 4.7b**—This regulation requires an electronic submission of a passenger and crew manifest, with specific data elements, to CBP 24-96 hours before arrival, depending on the length of the voyage.
  - **33 CFR 160—Notification of Arrival in U.S. Ports**—The Coast Guard changed its notification of arrival and departure requirements for vessels bound for or departing from ports or places in the United States. This rule requires electronic submission of cargo

manifest information to the Customs and Border Protection and requires additional crew and passenger information. Currently, owners, agents, masters, operators or persons in charge of a vessel bound for a U.S. port must file a NOA 96 hrs before they enter port.

- **Information Sharing Executive Orders and Policy documents**
  - **E.O. 12333—Strengthened Management of the Intelligence Community**—Executive Order 12333 was issued by President Reagan on December 4, 1981 in an effort to better effectuate the conduct of intelligence activities by the United States. As amended, this order lays out goals and direction for the national intelligence effort, and describes the roles and responsibilities of the different elements of the US intelligence community. It also lays out a framework for the conduct of intelligence activities. This E.O. defines U.S. intelligence activities and U.S. persons and provides the authorities under which each intelligence agency operates and the limitations imposed on that authority.
  - **E.O. 13356—*Strengthening the Sharing of Terrorism Information to Protect Americans***—defines "terrorism information" as all information collected produced or distributed by intelligence, law enforcement, military, homeland security or other U.S. Government activities related to foreign or international terrorist groups or individuals. EO 13356 also established an Information Systems Council, and requires the Attorney General, Secretary of DHS and Director of Central Intelligence to jointly establish requirements and guideline for the collection and sharing of terrorism information collected within the United States.
  - **E.O. 13388**—*Further Strengthening the Sharing of Terrorism Information to Protect Americans*.—The EO states that to the maximum extent consistent with applicable law, agencies shall, in the design and use of information systems and in the dissemination of information among agencies: (a) give the highest priority to (i) the detection, prevention, disruption, preemption, and mitigation of the effects of terrorist activities against the territory, people, and interests of the United States of America, (ii) the interchange of terrorism information among agencies, (iii) the interchange of terrorism information between agencies and appropriate authorities of States and local governments, and (iv) the protection of the ability of agencies to acquire additional such information; and (b) protect the freedom, information privacy, and other legal rights of Americans in the conduct of activities implementing subsection (a).
  - **Presidential Memorandum** for the Heads of Executive Departments and Agencies titled *Guidelines and Requirements in Support of the Information Sharing Environment* dated December 16, 2005.
  - **DoD 5240 1-R—Procedures Governing the Activities of DoD Intelligence Components that Affect United States Persons**—This DoD regulation sets forth procedures governing the activities of DoD intelligence components that affect U.S. persons Procedures 1-4, 14, and 15 set procedures for governing the activities of DoD intelligence components that affect U.S. persons. This Regulation is the sole authority by which DoD intelligence components may collect, retain, and disseminate information regarding U.S. persons. It specifically limits assistance to law enforcement authorities.. Among other things, this DoD regulation outlines the types of information that may be collected by a DoD intelligence component about U.S. persons. Procedures 1-4, 14, and

15 set procedures for governing the activities of DoD intelligence components that affect U.S. persons. This Regulation is the sole authority by which DoD intelligence components may collect, retain, and disseminate information regarding U.S. persons. It specifically limits assistance to law enforcement authorities.

- **DoD 8320.2—Data Sharing in a Net-Centric Department of Defense**—Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG). Data shall be made visible, accessible, and understandable to any potential user in the Department of Defense as early as possible in the life cycle to support mission objectives. Data assets shall be made visible and shall conform to the Department of Defense Discovery Metadata Specification. DoD metadata standards shall comply with applicable national and international consensus standards for metadata exchange whenever possible and all metadata shall be discoverable, searchable, and retrievable using DoD-wide capabilities. Data assets shall be made accessible and shall be accessible to all users in the Department of Defense except where limited by law, policy, or security classification. Data that is accessible to all users in DoD shall conform to DoD-specified data publication methods that are consistent with GIG enterprise and user technologies. Data assets shall be made understandable and shall have associated information assurance and security metadata.

Appendix C—Hub Functions

Vessel Hub

The following are examples of the functions that the Office of Naval Intelligence and Intelligence Coordination Center would accomplish in meeting the responsibilities associated with the National Maritime Intelligence Center and MDA Enterprise Hub for Vessels. MDA Hub functions that extend beyond current responsibilities will require additional or reprogrammed resource:

- Inventory and catalog world-wide vessel data that is available to the maritime community of interest;
- Identify legal, policy, cultural and other barriers to the sharing of vessel related information among the maritime community of interest. Make recommendation to improve the effective exchange of such information;
- Coordinate the acquisition and archiving efforts of both government and non-government data relating to vessel locations and background information; including Characteristics and Performance (C&P), owner and operator layers, vessel pedigree, operating network links, cargo, crew member, and passenger data. Additionally, events related to specific actions including but not limited to port calls, Maritime Interception Operations (MIO), suspicious behavior, and Illegal activity will be acquired through both government and non-government means for archiving and analysis. This effort will consolidate the purchases of commercial data with the goal of maximizing the depth and scope of the information, widening its dissemination, while minimizing the overall cost;
- Coordinate with the Architecture Management Hub the development of an Integrated Maritime Architecture (IMA) which will permit the maritime community of interest access and input to all available near-real-time and archived characteristics and positions of vessels on a global basis. This IMA effort will also provide the maritime community of interest with information regarding physical characteristics, ELINT parameters and ACINT data, photos, blueprints, and ownership information, and all other related data;
- Lead the effort to acquire identifying data for vessels less than 100 tons in conjunction with other organizations;
- Coordinate the development of expert systems which, based on vessel information (flag of registry, ownership and operating ties, cargo activity, crew composition, movement patterns, etc.), identify vessels exhibiting patterns which meet user defined profiles. Coordinate development of an alerting capability based on these same user profiles to notify the larger maritime community of interest. Such vessels will be referred for further ISR collection, enhanced background checks, or law enforcement action;
- Promote and implement data sharing standards which allow select vessel information and alerts to be displayed and disseminated to the right person, in the right place, and in the right format using a wide variety of systems in use throughout the federal government, the international community, civil agencies and private sector;

- Collaborate with the Architecture Management, Cargo, People and Infrastructure Enterprise Hubs to develop interfaces and data standards which allow these data sources to be integrated, fused, sorted and analyzed in a user defined display;
- Interface and participate with the technical development efforts on enhancing and replacing MDA systems which provide ever increasing levels of situational awareness regarding vessel information. The Enterprise Hub for Vessels will serve as the primary community advocate for developing systems which narrow or eliminate requirements gaps factoring in key variables such as qualitative advantages, cost, technical obstacles, training and manpower requirements. The objective of this activity is to continually reduce the size of the vessels that can be reliably detected and tracked while increasing the number and size of the coverage areas and the timeliness of the data;
- Facilitate and expedite the implementation of common vessel data and tracking standards. Encourage international vessels tracking efforts to develop vessel tracking systems compatible with agreed upon standards;
- Establish a set of common metrics to determine the level of performance for MDA systems supporting the Vessel Enterprise. Develop services based upon the established metrics for monitoring the measures of effectiveness of the Vessel Enterprise. Incorporate automated notification to operators and users if there is a disruption in the system or the supporting networks affecting the timeliness, completeness or accuracy of the data; and.
- Make recommendations for improving the performance, reliability, availability and survivability of the networks and system architecture supporting the Vessel Enterprise.

Cargo Hub

The following are examples of the functions that the U.S. Customs and Border Protection (CBP) would accomplish in meeting the responsibilities associated with the MDA Enterprise Hub for Cargo. MDA Hub functions that extend beyond current responsibilities will require additional or reprogrammed resource:

- Inventory and catalog worldwide cargo data that is available to the maritime community of interest;
- Identify legal, policy, cultural and other barriers to the sharing of cargo related information among the maritime community of interest. Make recommendation to improve the effective exchange of such information;
- Coordinate the acquisition and archiving efforts of both government and non-government data relating to cargo movement within the marine transportation system;
- Coordinate with the Architecture Management Hub and the International Trade Data System (ITDS) to permit the maritime community of interest access and input to all available cargo data;
- Coordinate the development of cargo analysis system(s) that identifies anomalies and allows for federated queries based on data-access levels;
- Promote and implement data sharing standards which allow cargo information and alerts to be displayed and disseminated to the right person, in the right place, and in the right format

using a wide variety of systems in use throughout the federal government, the international community, civil agencies and private sector;

- Collaborate with the Architecture Management, Vessel, People and Infrastructure Enterprise Hubs to develop interfaces and data standards which allow these data sources to be integrated, fused, sorted and analyzed in a user defined display;
- Interface and participate with the technical development efforts on enhancing and replacing MDA systems, which provide ever-increasing levels of situational awareness regarding cargo information;
- Facilitate and expedite the implementation of common cargo data standards;
- Encourage international cargo security standards by promoting the World Customs Organization (WCO) *Framework of Standards to Secure and Facilitate Global Trade* (Framework);
- Establish a set of common metrics to determine the level of performance for MDA systems supporting the Cargo Enterprise. Develop services based upon the established metrics for monitoring the measures of effectiveness of the Cargo Enterprise. Incorporate automated notification to operators and users if there is a disruption in the system or the supporting networks affecting the timeliness, completeness or accuracy of the data; and
- Make recommendations for improving the performance, reliability, availability and survivability of the networks and system architecture supporting the Cargo Enterprise.

People Hub

The following are examples of the functions that the U.S. Customs and Border Protection (CBP) would accomplish in meeting the responsibilities associated with the MDA Enterprise Hub for People. MDA Hub functions that extend beyond current responsibilities will require additional or reprogrammed resource:

- Inventory and catalog worldwide passenger/crew/transportation worker ("people") data that is available to the maritime community of interest;
- Identify legal, policy, cultural and other barriers to the sharing of people related information among the maritime community of interest. Make recommendation to improve the effective exchange of such information;
- Coordinate the acquisition and archiving efforts of both government and non-government data relating to people movement/employment within the marine transportation system;
- Coordinate with the Architecture Management Hub to permit the maritime community of interest access and input to all available people data;
- Coordinate the development of people analysis system(s) that identifies anomalies and allows for federated queries based on data-access levels;
- Promote and implement data sharing standards which allow people information and alerts to be displayed and disseminated to the right person, in the right place, and in the right format using a wide variety of systems in use throughout the federal government, the international community, civil agencies and private sector;

- Collaborate with the Architecture Management, Vessel, Cargo and Infrastructure Enterprise Hubs to develop interfaces and data standards which allow these data sources to be integrated, fused, sorted and analyzed in a user defined display;
- Interface and participate with the technical development efforts on enhancing and replacing MDA systems, which provide ever-increasing levels of situational awareness regarding people information;
- Facilitate and expedite the implementation of common people data standards;
- Encourage international maritime security standards by promoting the World Customs Organization (WCO) *Framework of Standards to Secure and Facilitate Global Trade* (Framework) and the International Maritime Organization (IMO) *Convention for the Suppression of Unlawful Acts Against the Safety of Maritime Navigation* (SUA);
- Establish a set of common metrics to determine the level of performance for MDA systems supporting the People Enterprise. Develop services based upon the established metrics for monitoring the measures of effectiveness of the People Enterprise. Incorporate automated notification to operators and users if there is a disruption in the system or the supporting networks affecting the timeliness, completeness or accuracy of the data; and
- Make recommendations for improving the performance, reliability, availability and survivability of the networks and system architecture supporting the People Enterprise.

Infrastructure Hub

The National Infrastructure Coordinating Center (NICC) will serve as the MDA enterprise Hub for infrastructure. The NICC is a 24x7 coordinating center for information, communications, and situational awareness covering the 17 critical infrastructure and key resource areas identified in HSPD-7 and the National Infrastructure Protection Plan (NIPP). In fulfilling its responsibilities as the infrastructure enterprise Hub, the NICC will draw upon resident experience in coordinating resources throughout the Department of Homeland Security's Office of Infrastructure Protection (OIP), including among others, the Infrastructure Coordination and Analysis Office (ICAO), the Risk Management Division (RMD), and the Homeland Infrastructure Threat and Risk Analysis Center (HITRAC). MDA Hub functions that extend beyond current responsibilities will require additional or reprogrammed resource.

Based on the functions of enterprise Hubs specified in section 11.1, the NICC will fulfill its responsibilities as the infrastructure Hub through the following specific actions:

- The NICC will build upon existing relationships with other government, private sector and international entities such as the Sector Coordinating Councils (SCCs), Government Coordinating Councils (GCCs), Sector Specific Agencies (SSAs), and Information Sharing and Analysis Centers (ISACs). Through these and other relationships, the NICC will bring together subject matter experts on maritime infrastructure to support maritime infrastructure domain awareness;
- The NICC will coordinate with applicable federal, sate, local, tribal, private sector and international elements, including the National Operations Center, the Transportation Security Administration, and the USCG;

- Provide suspicious activity reports relating to relevant infrastructure to appropriate federal, sate, local, tribal, private sector and international agencies, including HITRAC, DHS I&A, USCG MIFC, FBI counter-terrorism watch, and TSA Intelligence Service (TSIS);
- Coordinate responses to requests for information on critical infrastructure among government and private industry;
- Provide information and situational awareness of related infrastructures which significantly impact maritime infrastructure and operations such as multi-modal transportation, electricity, telecommunications, and information technology;
- Coordinate with maritime subject matter experts to catalog data sources and define access requirements to those resources;
- Continuously monitor identified government, private sector, and commercially procured online resources;
- Build upon existing operational relationships with information centers and identify any additional relationships necessary to achieve MDA;
- Leverage operational relationships to identify and understand databases, web portals, and other information sources available to achieve and maintain MDA.
- Maintain situational awareness of related critical infrastructures which may impact or be impacted by incidents involving maritime infrastructure (e.g. electric power, transportation interconnections, refineries, grain elevators, etc.);
    - Coordinate with appropriate agencies within the DHS Office of Infrastructure Protection,
    - Coordinate with designated sector-specific agencies as defined in the National Infrastructure Protection Plan;
- Identify governmental and commercially-available sources of maritime infrastructure information;
- Conduct a gap analysis of required additional information and recommend a course of action to acquire missing elements of information;
- Leverage existing governance and policy organizations to identify maritime infrastructure information sources capable of providing information elements for each defined level of awareness. Initiate working group(s) with subject matter experts from the identified sources to catalog current sources for the information elements;
- Work with the architecture enterprise Hub to enable respective owners of identified information to provide and update their information directly to the infrastructure Hub;
- The NICC will collect and document progress toward the goals in this document. Working with the infrastructure enterprise working group, the NICC will identify any policy, technology, or other obstacles to achieving MDA as defined in Appendix D;
    - There are several obstacles immediately apparent, including,
        - Possible legal and policy restrictions to the sharing of infrastructure-related information, including restrictions of public-private information exchange, sharing of

classified material, Protected Critical Infrastructure Information (PCII) and other industry or government sensitive data,

- The NICC is almost exclusively focused on domestic critical infrastructure and will therefore in the near term have limited ability to provide situational awareness of maritime infrastructure worldwide. New partnerships will be essential to gaining and maintaining worldwide MDA infrastructure awareness,
- There is currently no consolidated compilation for maritime infrastructure suspicious activity and threat reporting. The NICC can leverage membership in the Information Sharing Environment (ISE) suspicious activity working group and relationships with HITRAC and MIFC maritime analysts to work toward information transparency for analytical organizations,
- Personnel and/or capital resource requirements to fulfill the MDA infrastructure enterprise Hub mission have not yet been clearly analyzed, nor is funding currently secured to meet those requirements.

- Identify near-term enhancements to existing supporting technology to facilitate easier and broader information sharing within the MDA team;
- Ensure Enterprise Hub leads are aware of PCII and other industry information sharing sensitivities;
- Develop rapid notification protocols for MDA stakeholders in the event of a significant incident involving maritime infrastructure; and
- Ensure critical infrastructure reporting, including DHS situational reporting and NICC-generated Spot and Situation Reports, are provided to all enterprise Hub leads and other relevant stakeholders.