MARITIME DOMAIN AWARENESS ARCHITECTURE MANAGEMENT HUB PLAN

Department of the Navy | Chief Information Officer

Report Documentation Page

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE **JAN 2009**	2. REPORT TYPE	3. DATES COVERED **00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE **Maritime Domain Awareness Architecture Management Hub Plan V1.2**	5a. CONTRACT NUMBER
	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Office of the Chief Information Officer,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**30**	

"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."

"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.

"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."

— National Plan to Achieve Maritime Domain Awareness

Information sharing is a foundational tenet of Maritime Domain Awareness (MDA). Currently, identical information is collected and stored by multiple agencies and organizations. However, these agencies are often unaware that similar information is available from other organizations, or they are aware but unable to share this information with one another because information sharing standards, agreements, policies, or processes currently do not exist. Similarly, agencies with relevant, related, or complementary information are unable to combine their data to achieve greater levels of situational awareness.

MDA is being implemented within the context of national information and data sharing guidance. This guidance includes Executive Order 13388 and the National Strategy for Information Sharing (references (k) and (i)). The National Strategy for Information Sharing, although broader in scope than just MDA and focused on terrorist information, establishes guiding principles and foundational elements for information sharing on a national level. Many other policies, guidance documents, strategies, and plans (see References section at end of document) help set and shape the direction of information sharing for the Global Maritime Community of Interest (GMCOI) and are discussed throughout this document. They play a major role in establishing mechanisms for collaborating and enabling an aligned transition to the desired information sharing state for the GMCOI.

The National Concept of Operations for Maritime Domain Awareness (MDA CONOPS) (reference (c)) describes this desired state as an environment in which the GMCOI embraces and achieves the common objective of obtaining and sharing information as a mechanism to increase the safety, security, and economic prosperity in the maritime domain.

The MDA CONOPS outlines how the Federal Government will organize to achieve maritime domain awareness. It creates a federal interagency structure that includes an MDA Stakeholder Board to coordinate and align MDA policies. In addition, the MDA CONOPS creates four enterprise hubs. Each of these hubs is responsible for coordinating information sharing among the multiple agencies and organizations within each MDA information pillar: vessels, cargo, people, and infrastructure.

An additional hub, the Architecture Management Hub, was established by the MDA CONOPS to design and manage the overall enterprise architecture needed to facilitate net-centric sharing of maritime information among the GMCOI as described in the MDA CONOPS. An enterprise architecture provides a clear and comprehensive picture of the structure of an entity, whether an organization, functional area, or mission area. It provides those who manage, construct, and maintain the entity with a clear and understandable picture of the entity's uses, features, functions, and supporting systems, including relevant standards. The MDA enterprise architecture will provide the standards and processes that will allow the four enterprise hubs, and any other maritime community member, to share information and services.

The MDA CONOPS identifies a lead agency or department for each of the four enterprise hubs and the Architecture Management Hub. The Department of the Navy (DON) is the executive agent for the Department of Defense for MDA and has been designated as the lead department for the Architecture Management Hub. The DON has further delegated this responsibility to the Department of the Navy Chief Information Officer (DON CIO).

This document provides an initial high-level plan for carrying out the responsibilities of the national Maritime Domain Awareness Architecture Management Hub to deliver a standards based service oriented architecture that will align MDA capabilities.

It outlines key goals of the MDA Architecture Management Hub and how the hub will build on previous, current, and emerging information sharing initiatives. A discussion of necessary governance in the context of the MDA Architecture Management Hub follows. Subsequently, high-level strategies for the overall MDA enterprise architecture, as well as strategies for key tenets of net-centric information sharing (data standards and information assurance) are included. Finally, this document will address the resource implications for development and implementation of the architecture.

Goal

The goal of the Architecture Management Hub is to provide a blueprint to develop a net-centric, information sharing environment, in which data from disparate sources and security domains will be discoverable, accessible, understandable, fused, and usable, with appropriate information assurance, to enable user defined and common operational pictures. This blueprint will guide departments and agencies in their development of capabilities to enable MDA, and facilitate the sharing of maritime information with state, local, and tribal governments, international partners, and the private sector.

The principal characteristic of the MDA enterprise architecture is that it will be actionable. As an actionable architecture, it will:

- Inform relevant investment decisions.
- Translate stakeholders' capability needs into requirements that can be engineered.
- Drive the design of services, applications, and systems based on those requirements.
- Support the selection of technology that fulfills capability needs.
- Provide a formal basis for validating solutions

against the originally identified capability needs.

Vessel Positions in the Mediterranean Sea

Building on Current Initiatives

Interagency involvement in the development of the architecture will be critical to obtaining support for, and use of, the architecture. The authority to direct MDA stakeholders to publish data and make services available resides within the components and agencies themselves. As a result, articulating the benefits of a networked, Service Oriented Architecture (SOA) and demonstrating early accomplishments will be critical to the long term success of the effort (SOA is discussed in more detail on page 10). Development of the architecture will proceed in an incremental fashion with new users and services added over time, including those from state, local, and tribal governments, the pri-

vate sector, and international partners.

The efforts of the Architecture Management Hub will build on earlier accomplishments of the MDA Implementation Team and its associated work groups. In 2007 the MDA Implementation Team established an on-going national MDA organizational structure through the MDA CONOPS. The MDA Implementation Team also used a four-step capability-based assessment process to document initial requirements and existing capability gaps for MDA. These documents include: the Interagency Requirements Analysis (reference (e)), Interagency Needs Analysis (reference (f)), Interagency Capabilities Document (reference (g)),

and Interagency Investment Strategy (reference (d)). These documents identify 15 critical capability gaps and the tasks required to fill them. Of these tasks, the following three relate to net-centric information-sharing:

- Enable network access to all designated nodes across the GMCOI.
- Implement Information Assurance (IA) and Cross Domain Security procedures across the GMCOI.
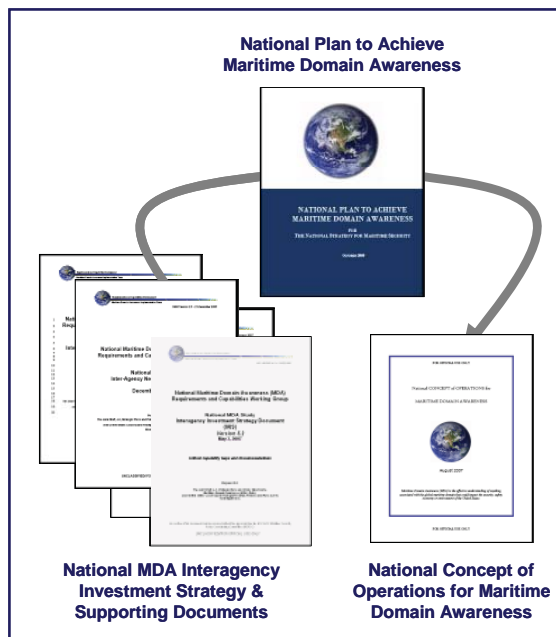- Establish National MDA data standards across the GMCOI.

These tasks, along with the recommended solutions, will provide the initial priorities for the MDA enterprise architecture.

The MDA Interagency Core Architecture Document (IACA) (reference (h)), developed as part of this work, provided a preliminary look at both as-is and to-be elements of an interagency MDA enterprise architecture. The IACA development process focused on identifying existing, or as-is interagency relationships and current MDA capabilities and gaps. This development process also identified possible courses of action for agency and departmental decision makers to close current capability gaps as part of the to-be architecture efforts.

Within the MDA community, other initiatives are underway to develop net-centric capabilities. Ground breaking efforts, such as the MDA Data Sharing Community of Interest (DS COI), have led the way in developing SOA capabilities within the MDA community. The goal of these efforts has been to make maritime data discoverable (easy to find), accessible, understandable, and usable for a variety of users, including those who previously could not obtain and make use of the data. The MDA DS COI has made data and services available for use by other applications using DoD's Net-Centric Enterprise Services and has provided an interface for the unanticipated user via a Google Maps Mediation Service.

The Office of Naval Intelligence is using a phased approach to transition and transform the Integrated Maritime Intelligence Architecture (IMA) to an enterprise architecture that optimizes functional and technological capabilities to enable seamless and scalable access to an integrated global maritime intelligence domain. The IMA will implement a SOA approach "for organizing and (re) using enterprise services to support interoperability between National Maritime Intelligence Center enterprise data assets and applications, and established data sharing and interoperability environments with DoD, federal, and Coalition partners" (reference u).

MDA Implementation Team Family of Documents

The National Oceanographic and Atmospheric Administration (NOAA) is leading an effort to develop a coordinated national network of ocean, coastal, and Great Lakes observation capabilities known as the Integrated Ocean Observing System (IOOS). IOOS represents a national partnership of 17 federal agencies and 11 regional associations sharing responsibility for the design and operation of the system. Once completed, IOOS will integrate oceanographic observation systems from throughout the federal, state, and local governments, as well as the scientific and academic communities. IOOS has already made tremendous strides sharing maritime information across widely dispersed agencies and organizations that will greatly benefit the Architecture Management Hub effort.

Of particular note is the interagency work being accomplished for the Federal Information Sharing Environment (ISE). Although the ISE is primarily concerned with sharing terrorist related information, their effort, "…aligns and leverages existing
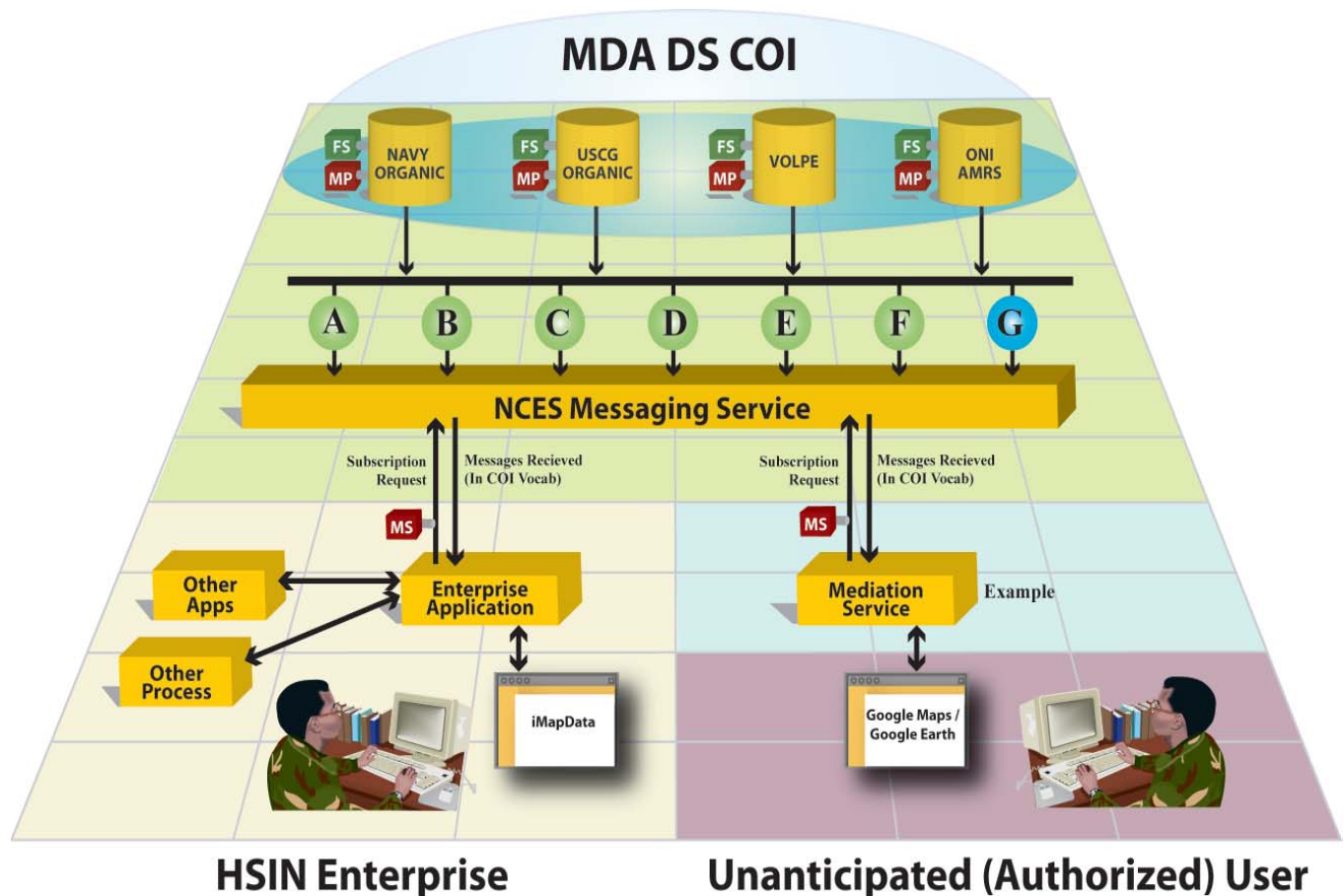
information sharing policies, business processes, technologies, systems, and promotes a culture of information sharing through increased collaboration" (reference (J)). These same areas must be aligned to form a cohesive enterprise architecture for MDA.

The Architecture Management Hub will build on the successes of these efforts, while encouraging other successful MDA efforts, including numerous international efforts, to integrate into the net-centric environment. Many current efforts provide a tremendous capability, but exchange information in a point-to-point manner and do not benefit the broader maritime community. Once these capabilities are migrated to a SOA, their data and services can be re-used and made available to any authorized user as necessary to enable MDA.

These various efforts are being developed and fielded without a unifying architecture to form a cohesive information sharing environment that can benefit all partners in the GMCOI. The Architecture Management Hub will align these and other efforts, identify and catalogue relevant associated systems, and leverage the standards and processes that already exist. This will help to establish a comprehensive current state architecture MDA related efforts. Based on this work, transition and implementation plans will be developed to achieve the desired end-state MDA enterprise architecture.

As the Architecture Management Hub matures, metrics and measures of effectiveness will be developed to ensure sufficient progress is being made toward its objectives. Various existing operational exercises will be used to evaluate the ability of users to exchange information. A concerted outreach effort will also be undertaken to inform and educate potential users on the processes developed and how to participate in the network.

MDA DS COI Spiral 1 Architecture Representation

As the lead for the Architecture Management Hub, the DON CIO will work with the existing governance structure established by the MDA CONOPS, and will leverage other governance bodies, such as the Federal CIO Council. In this role, the DON CIO will focus on coordinating the MDA enterprise architecture efforts and developing appropriate policies, procedures, and standards.
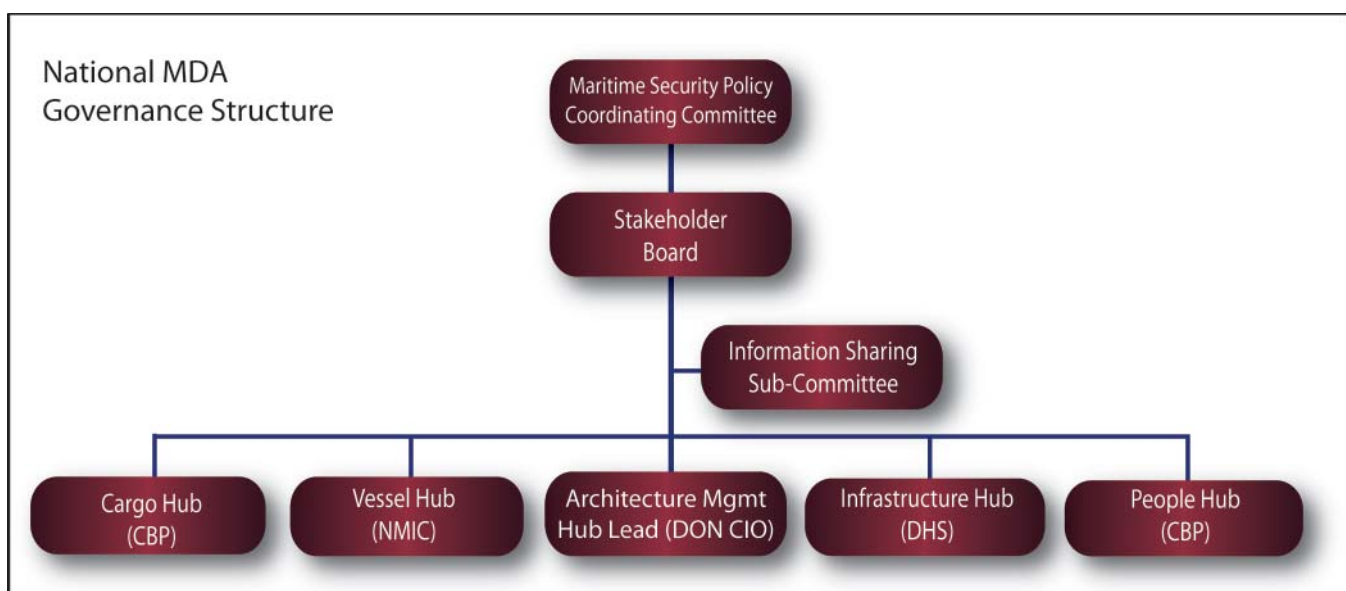
Federal interagency MDA efforts are coordinated by the MDA Stakeholder Board, which is co-chaired by the Director, Global Maritime and Air Intelligence Integration (GMAII) and Director, Global Maritime Situation Awareness (GMSA). The Stakeholder Board is a coordinating body under the Maritime Security Policy Coordination Committee, and is responsible for MDA policy alignment, synergy, and issue resolution. The MDA Stakeholder Board will provide executive oversight of the Architecture Management Hub, and the four enterprise hubs (Vessel, Cargo, People, and Infrastructure). The Architecture Management Hub will work closely with the Information Sharing Sub-Committee (ISSC), which is the executive management and advisory body for maritime domain-related information sharing and technology issues.
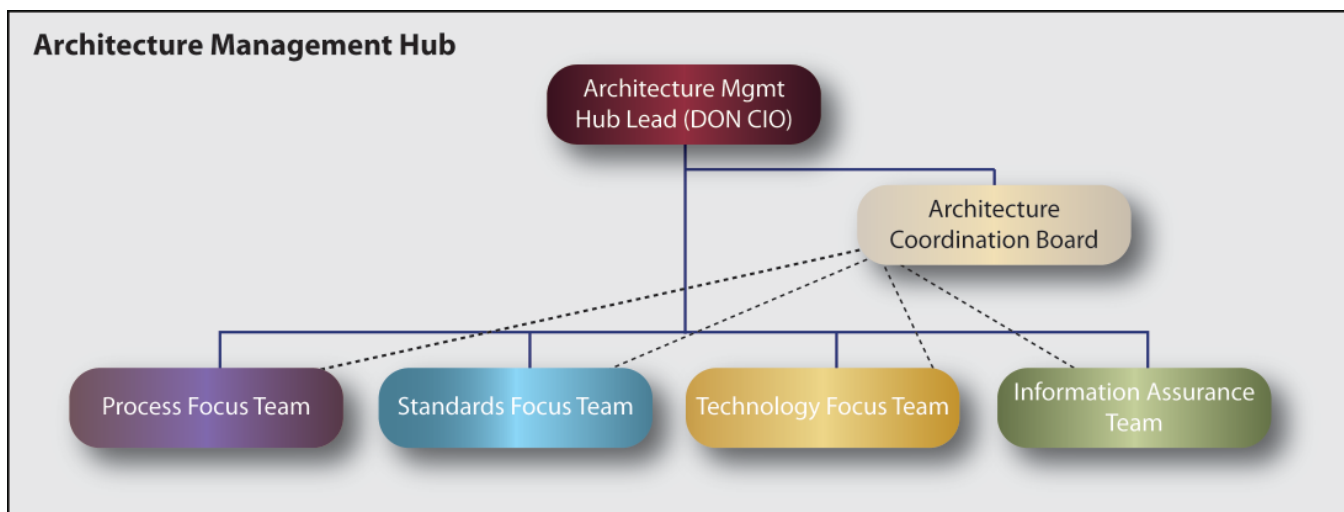
These governance structures will be leveraged to govern the necessary processes and service level agreements requisite for efficient, effective operation of an MDA enterprise architecture. In addition, the Architecture Hub will coordinate with the Federal CIO Council to ensure that the relevant information technology activities within the individual agencies are aligned to achieve MDA objectives.

The Architecture Management Hub, working with the ISSC, will identify policy barriers as well as cultural, procedural, and technological barriers to information sharing. Barriers include issues such as the lack of interagency coordination/alignment of information sharing policies, and a reluctance by some data providers to provide detailed information.

To effectively execute the roles and responsibilities of the Architecture Management Hub, the DON CIO will establish focus teams to concentrate on key aspects of the MDA enterprise architecture. Focus team leads will be designated by the DON CIO and membership will be composed of representatives from departments, agencies, and organizations with membership on the MDA Stakeholder Board. Focus team membership will eventually be expanded to include representatives from state, local, and tribal governments, international partners, and the private sector. Active participation by individuals with knowledge of information sharing ef-

National MDA Governance Structure

- Maritime Security Policy Coordinating Committee
- Stakeholder Board
- Information Sharing Sub-Committee
- Cargo Hub (CBP)
- Vessel Hub (NMIC)
- Architecture Mgmt Hub Lead (DON CIO)
- Infrastructure Hub (DHS)
- People Hub (CBP)

Architecture Management Hub

- Architecture Mgmt Hub Lead (DON CIO)
- Architecture Coordination Board
- Process Focus Team
- Standards Focus Team
- Technology Focus Team
- Information Assurance Team

Proposed Architecture Management Hub Structure

forts within their own agency and the expertise to effectively assist the focus team on its assigned task is critical. Initial focus teams will include: Process, Standards, Technical, and Information Assurance.

The Process Focus Team will document the MDA operational processes described in the MDA CONOPS and other documentation. They will also develop standard, non-technical processes and procedures for publishing and subscribing information to and from the network.

The Standards Focus Team will develop those standards (schema/vocabulary, metadata, etc.) that will allow users to publish data to the network and make it available to other users (subscribers). These standards will incorporate appropriate existing and emergent standards (e.g., UCore, NIEM, etc.) or procedures for mediation as necessary.

The Technology Focus Team will identify and recommend technical solutions to enable net-centric information sharing within the GMCOI.

The Information Assurance Focus Team will develop methods for protecting information published to the network, including methods to ensure only authorized users have access to information (confidentiality), information cannot be manipulated without authority (integrity), only authorized information is published to the network (authenticity), and information is available when needed (availability).
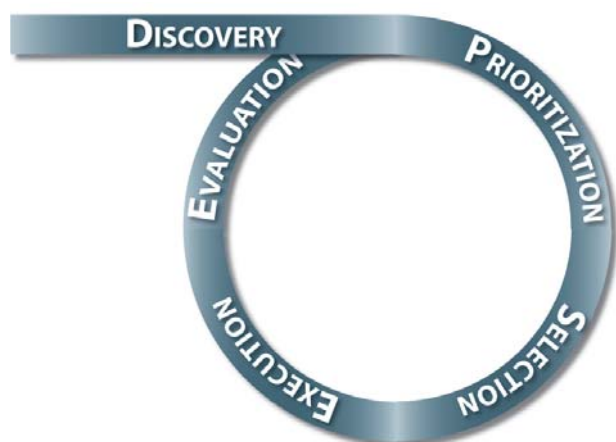
Each focus team will in effect be developing a part of the overall MDA enterprise architecture. To ensure synthesis of these parts and create an integrated, cohesive, and actionable enterprise architecture, an Architecture Coordination Board will be established. This board will be responsible for developing and recommending an MDA enterprise architecture description from the recommendations of the focus teams.

An iterative approach will be used to design the MDA enterprise architecture. In this way users of the architecture can realize early benefits during the design, and continue to see increased utility over time. Each of the Architecture Management Hub focus teams, guided by the Architecture Coordination Board, will explore topics within its scope, prioritize and select issues to address, work to resolve those issues, and evaluate the results before moving on. Focus teams will work in parallel on complementary issues where appropriate.

Steps in the Iterative Process

Discovery of Ongoing Relevant Efforts

The first step in the process will be a discovery phase in which the focus team works to understand relevant efforts already underway. Within this phase, the focus team will examine various aspects of these efforts including the scope, purpose, intended users, organizational roles and relationships, environments, and types of data/ information to be exchanged as applicable. In addition, the focus teams will need to review the level of effort, extent of capabilities, status of deliverables, and schedule. To some extent, initial discovery of relevant efforts has already been ongoing.

Prioritization

After building an understanding of the other relevant efforts, each focus team will prioritize the challenges within its scope based on gap analysis and input from the enterprise hubs. The focus teams will develop a prioritized list of actionable efforts to choose from, including potential courses of action.

Selection

Once a prioritized list is developed an issue will be chosen for the focus team to resolve. Guided by the MDA Stakeholder Board, each focus team will select the best option to pursue for its initial work from the prioritized list.

Execution

Based on the selection decision, each focus team will carry out its work to execute the selected effort. Ideally each focus team will work on one issue at a time in a logical sequence, but parallel efforts may be necessary.

Evaluation

Once the initial effort is completed, each focus team will evaluate the results, and with the assistance of the Architecture Coordination Board, incorporate them into the architecture. Following this, the focus team will update its gap analysis and plan for the next iteration. In addition the focus team will develop a sustainment plan to ensure the longevity of the solution that was developed.

The principal characteristic of the MDA enterprise architecture is that it will be actionable. It will be developed and delivered as three principal products:

- An As-Is Architecture Description describing the architecture of operations and resources that compose the current state of the MDA enterprise architecture.
- A To-Be Architecture Description describing the architecture of operations and resources that will compose the desired state of the MDA enterprise architecture.
- An Architecture Migration and Implementation Plan describing the capability gaps between the current (as-is) and desired states (to-be) of the MDA enterprise architecture as well as a plan for migrating existing resources and for developing new resources in response.

The as-is and to-be architecture descriptions will be composed of variations of four primary models:

- An Operational Model focused on describing operational nodes and processes to share information within the GMCOI.
- An Information Model focused on enumerating and classifying the information exchanges with and within the GMCOI.
- An Interoperability Model focused on describing standards for the connection and exchange of information between information services.
- A Services Model focused on describing and classifying the information services necessary to facilitate the information exchanges.

Although each of the Architecture Management Hub focus teams will be exploring numerous aspects of their respective subject area and producing a variety of architectural and programmatic insights, their collective products will be integrated by the Architecture Coordination Board to form the four primary architectural models described in this section.

Operational Model. Preparatory to understanding the information exchanges and related services that describe the provisioning of capabilities for MDA information sharing, it is necessary to understand the larger operational context for such capabilities. This is accomplished by developing an operational model to describe operational processes and associated nodes for sharing information within the GMCOI.

The Operational Model will focus on operational processes that involve data and facilitate information sharing. The MDA CONOPS provides an initial high level categorization of these operational processes as: Monitor, Collect, Fuse, Analyze and Disseminate. MDA stakeholder segment architectures (as available) can be aligned to these operational processes to build an integrated operational model for MDA.

Information Model. The key to developing an actionable MDA enterprise architecture is a complete and correct understanding of the information necessary to support the operations and processes described in the MDA CONOPS. This is accomplished by developing an information model that enumerates and classifies the information exchanges with and within the GMCOI.

This will include:

- Planned exchanges between MDA information pillars, i.e. vessels, cargo, people, and infrastructure pillars.
- Unplanned or unanticipated exchanges between MDA information pillars.
- Planned and unplanned exchanges between MDA information pillars and external entities, e.g. non-GMCOI mission area organizations.

The resulting understanding provides the foundation for all other MDA information sharing architecture development.

Interoperability Model. Architectural styles, such as Service-Oriented Architecture (SOA), depend on the use of standard protocols to enforce the principles, practices, and patterns composing the style. In the case of SOA, these protocols standardize the way information services connect and exchange information via service interfaces. The use of such protocols ensures interoperability as solution elements are developed and deployed to create

the MDA enterprise architecture. This is accomplished by developing an interoperability model focused on describing standards for the connection and exchange of information between information services.

Services Model. The information exchanges described earlier can be viewed as the provisioning of capabilities among and by the entities composing the GMCOI. Best practices in architecture dictate the use of a service-oriented model to describe this provisioning of capabilities. In other words, emphasis is upon services as the providers of capabilities to consumers. This is accomplished by developing a services model focused on describing and classifying the information services necessary to facilitate the information exchanges. This is in contrast to traditional approaches to information systems architecture that focus on the underlying hardware and software as the solution to capability need. The development of a services model implies the use of an SOA architectural style.
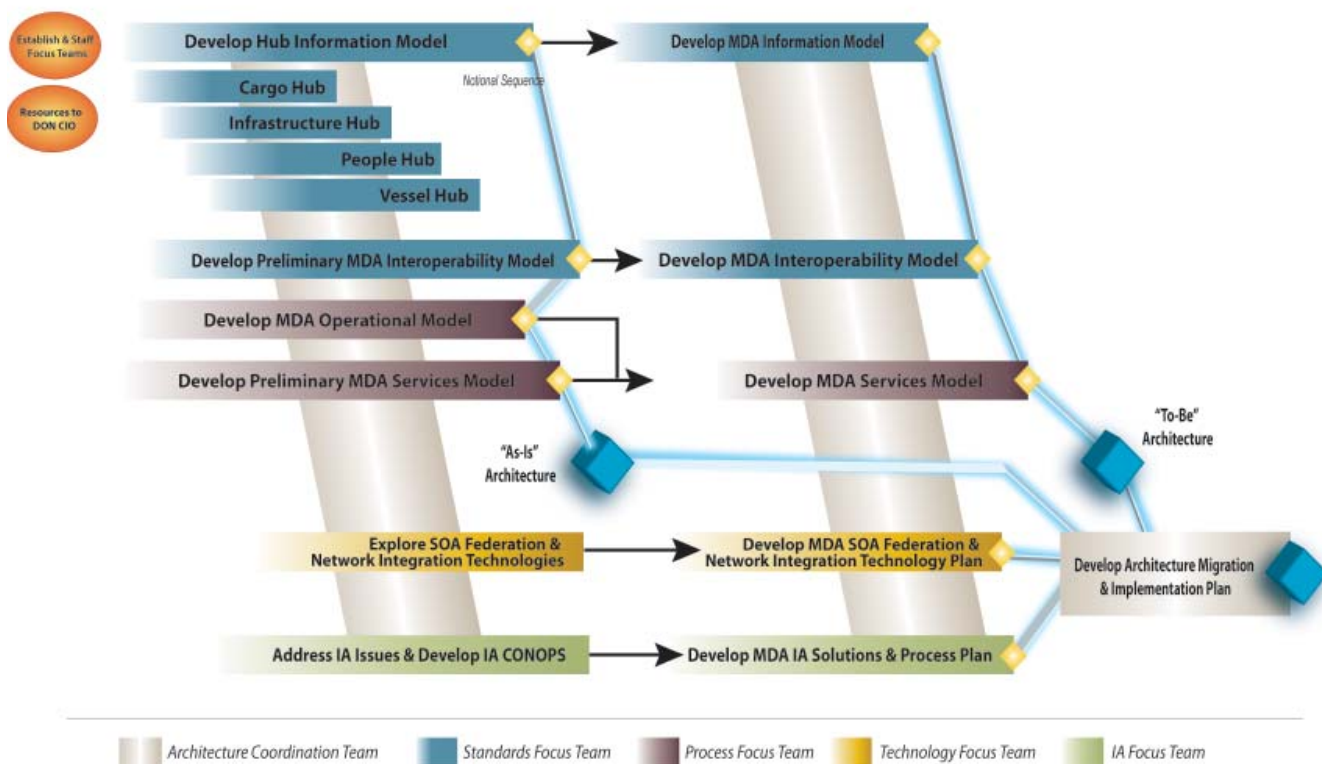
The following diagram provides a high level outline of these four models as milestones to achieve the as-is architecture and an initial version of the to-be architecture

There are two key aspects that must be considered in developing the above models. The first is the employment of SOA principles, practices, and patterns. The second is the use of architecture description artifacts mandated by accepted architecture frameworks. The following discussion addresses the importance of these considerations in creation of the MDA Enterprise Architecture.

Service-Oriented Architecture

It is important to separate the issues of service-oriented architecture from service-oriented implementation and the use of associated technologies. SOA focuses on how to design the provisioning of automated capabilities and the interaction of architectural entities (i.e. services) that provide such capabilities. Service-oriented implementation focuses on the design of technical solutions that implement automated functions to achieve a service-oriented architecture. The four models described above will focus on SOA, but an effective MDA information sharing solution will also require evaluation and development of technology for service-oriented implementation.

The Technology Focus Team will explore exist-

MDA Architecture Increment 1.0 FY09-FY10 High Level Development Plan

ing infrastructure available to the GMCOI in search of capabilities to satisfy the emerging infrastructure service requirements described in the services and information exchange models. The team will identify capability gaps, plan for solutions, and develop a solution architecture that identifies the use of existing and needed technologies to achieve the MDA enterprise architecture.

From a SOA point of view, this would include evaluation of enterprise service infrastructures and catalogs of available services resident in registries and repositories distributed throughout the GMCOI. It is important that the capabilities available via the MDA information pillars adhere to the interoperability model and make discoverable, available, and usable their current and future information services to satisfy the services and information exchange models. Evaluation and mapping of current capabilities within the GMCOI will result in development of an as-is architecture for MDA information sharing.

Rather than architecting and constructing new technical solutions to achieve a to-be MDA enterprise architecture, existing capabilities and technology will be federated, or linked, to create new capabilities. Through its focus teams, the Architecture Management Hub will identify existing architecture federation approaches, recommend a federation strategy, and transition legacy technology to a federated approach where existing capabilities or services within organizations are able to interact.

Numerous efforts are ongoing throughout the Federal Government to develop core enterprise infrastructure and services. Core services commonly include directory and search capability, identity management services and attribute stores, security services, mediation, messaging, and collaboration.

Exposing, leveraging, and aligning these services will be critical to the MDA enterprise architecture. The challenge to the Architecture Management Hub will be to federate these infrastructures to facilitate net-centric information sharing between federal departments and agencies, state, local, and tribal governments, international partners and the private sector. Although some work has been done in the field of federated services, most notably by the Information Sharing Environment, this is basically a new business model. Federating service infrastructures will require the federation of core services where possible. For example, rather than develop an MDA metadata registry and repository, metadata registries from the various service infrastructures could be federated, thus allowing them to exchange information directly.
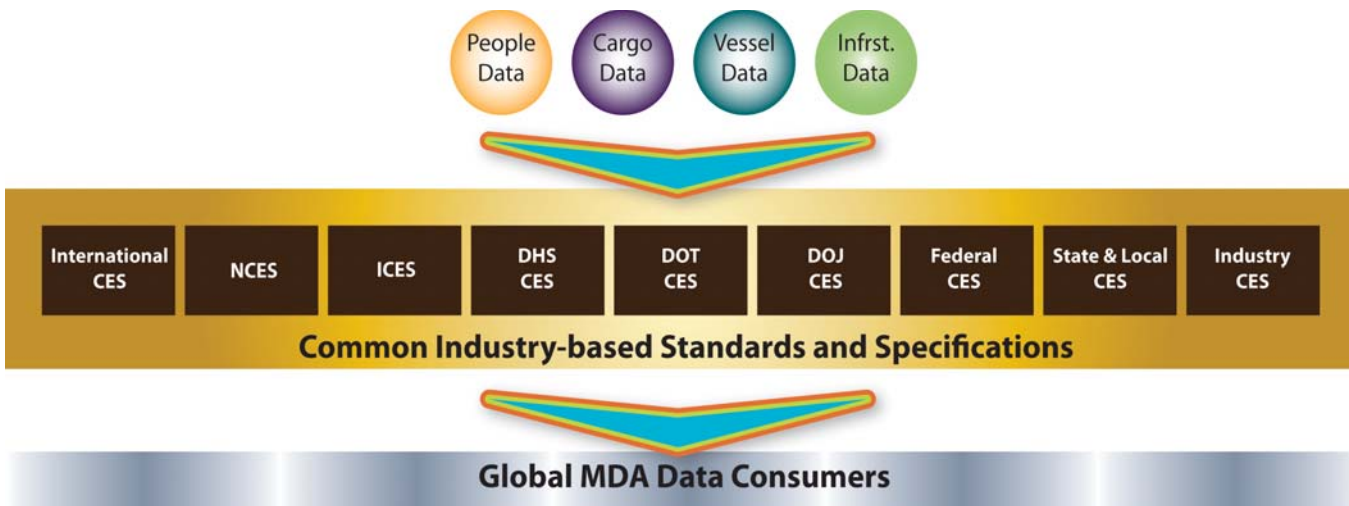
The challenge for the Architecture Management Hub will be to develop a repeatable process to federate services and infrastructures. The Architecture Management Hub will then need to educate members of the GMCOI on how to implement these processes. This can be done in an iterative approach in which users are continually trained as they are added to the network.

Because many federal departments and agencies do not yet operate in a net-centric SOA environment, an additional challenge for the Architecture Management Hub will be the need to provide methods for those agencies to publish and subscribe data and services to and from the network.

There will likely be some core services for which federation is not an optimal solution. Selection of an individual agency to provide these services to the GMCOI may be required. For instance, it may be necessary to select an "implementation agent" for some collaboration services to support a common operational picture across MDA.

Architecture Frameworks and Descriptions

Once completed, the MDA enterprise architecture must be presented in a form commonly used by and understandable to decision-makers, reviewers, and architects of other efforts. This is usually accomplished through the use of an architecture framework - a framework for describing and communicating architectures. Such a framework is a set of assumptions, concepts, values, and practices

Common Standards and Specifications to Facilitate Information Sharing Across the Infrastructures

that constitutes a way of viewing an architecture reality. An architecture framework provides a collection of patterns for creating and presenting architecture descriptions.

There are three architecture frameworks of interest in the development of the MDA enterprise architecture: the Federal Enterprise Architecture (FEA); the DoD Architecture Framework (DoDAF); and the Information Sharing Environment Enterprise Architecture Framework (ISE EAF).

Most non-DoD federal agencies employ the FEA and its recent extension, the Federal Segment Architecture Methodology (FSAM). FEA emphasizes the use of architectural element taxonomies expressed as references models (e.g. Business Reference Model, Data Reference Model, Service Component Reference Model, etc.). To ensure maximum interagency application, the Architecture Management Hub will utilize the Federal Enterprise Architecture in describing the MDA enterprise architecture.

DoD commands, services, and agencies, as well as the Coast Guard, employ the DoDAF. DoDAF emphasizes the use of a variety of architectural models to describe differing perspectives or views of a whole architecture. DoDAF provides a formal nomenclature for such models. Embedded within the FEA is the idea of using models to express architectural elements and their relationships. Although FEA and DoDAF use similar models, FEA does not specify a model nomenclature.

The challenge to the Architecture Management

Hub will be to integrate the use of models common to both FEA and DoDAF within the higher-order structure of the FEA's taxonomies to create an actionable architecture description for the MDA enterprise architecture.

While the FEA and the DODAF are compliance frameworks, the ISE EAF is not vested in policy as required for compliance. Rather, the ISE EAF provides constructs, or patterns, for sharing information at the federal level.

The Information Sharing Initiative ISE EAF was developed by the PM-ISE. The ISE and the information resources construct developed from the ISE EAF, will link ISE participants (federal, state, local and tribal governments, foreign partners and allies, and the private sector) to create a distributed, protected, and trusted environment for sharing information. The ISE EAF will evolve over time as additional business processes, information flows and exchanges, services, and technologies are defined and incorporated into the ISE. While the ISE EAF was developed for primary use as a tool for anti-terrorism, its constructs can be used to enable general information sharing within the Federal Government.

Vision for Net-Centric Data and Services Sharing

Establishing a shared vision for net-centric data and services sharing compels a shift from point-to-point interfaces to a many-to-many exchange of data, and enables many users and applications to leverage the same data and services. A key objective is to accelerate decision cycles by ensuring that the right data is available at the right time, in the right place.

Making data visible, accessible, understandable, and trustable are the cornerstones of net-centric information sharing. The creation of duplicative data and redundant capabilities often results from consumers' inability to locate, access, or understand existing data assets, or trust that they meet their needs.

The purpose of establishing data standards is to facilitate agile information sharing across the MDA community of data producers and data consumers.

The National MDA Architecture Management Hub's approach to data standards is to leverage existing data sharing initiatives, best practices, and lessons learned; identify information exchanges; identify authoritative sources of data as necessary;

The Ability to Publish and Subscribe is Key to Infrastructure Sharing

define data quality of service standards; and recommend common vocabulary, information exchange, and registration processes and tools. The goal of this approach is to provide seamless interoperability across the MDA community that will provide a secure, collaborative, information-sharing environment.
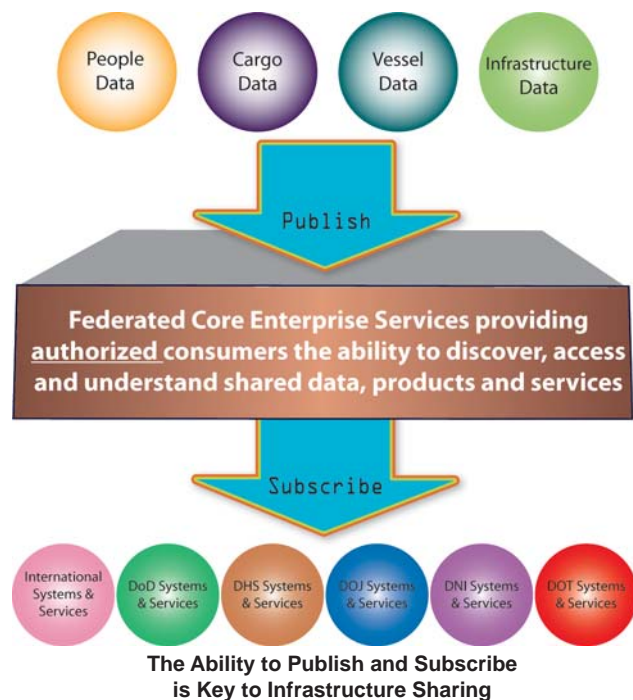
Reference Data and Services Synchronization

The MDA as-is data architecture will describe existing maritime data sources, producers, consumers, and existing information exchanges as a baseline for moving forward. Identifying existing data sharing initiatives, best practices, lessons learned, and information exchanges are critical early steps to creating the baseline. This baseline will assist in identifying data assets that are authoritative sources for data, as well as identifying the contexts in which the data is authoritative. In situations where there is more than one authoritative source, depending on how the data is used, services are needed to indicate the business process for which the authority is valid. Stewardship of data sources will be considered when determining authoritativeness.

A web-accessible registry will be needed to capture and manage data sources, producers, and consumers. As data producers register their data assets in the registry, the registry can be used to identify authoritative sources of data as necessary, reduce and eliminate duplicative data as appropriate, identify data gaps and incompatibilities, and align data naming, design, and information exchange standards.

Data Quality

Data assets can be trusted only if their contents are sufficiently accurate and of sufficiently reliable quality. Quality assertions about data include information on its accuracy, completeness, or timeliness for a particular purpose. For example, consumers might need to know the age of the data to determine whether it is still applicable, or they might need to know how accurate estimates and figures within the data asset are. Assessing and im-

proving data asset quality is important. Quality of service standards and active stewardship need to be defined and coordinated to establish and maintain the quality and relevance of authoritative data sources.

The Architecture Management Hub will: develop an ongoing process for the enterprise hubs to audit the quality of data assets that are made visible and accessible; develop guidelines for data producers and consumers to ensure that the data required by the GMCOI is available, accurate, complete, and interoperable; provide a single joint collaborative forum for coordination of MDA data architecture, data quality, and metadata; and provide a single means to address, resolve, and track data issues.

Standard Vocabulary Methodology

MDA data and services producers and consumers comprise a collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes. To facilitate this information exchange, the MDA users need a shared vocabulary for the information they exchange. The Architecture Management Hub will work with the Cargo, Vessel, People, and Infrastructure hubs to create necessary data standards and a shared vocabulary to facilitate exchange of the information within and among the hubs.

The National Information Exchange Model (NIEM), Universal Core (UCore), and Maritime Information Exchange Model (MIEM) are reference models designed to enable a level of interoperability in the exchange of information—for the sender and receiver of information to share a common, unambiguous understanding of the meaning of that information. Each of these reference models started independently but they are now aligning as complementary initiatives with complementary models.
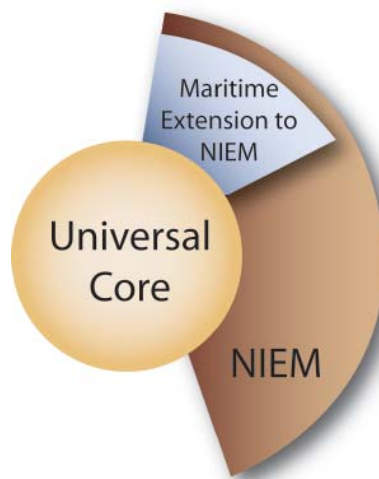
The NIEM "is designed to develop, disseminate, and support enterprise-wide information sharing standards and processes across the whole of the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise at all levels and across all branches of government" (reference (m)). The NIEM represents a collaborative partnership of agencies and organiza-

tions across all levels of government (federal, state, tribal, and local) and with the private sector.

The NIEM reference model includes two categories of reusable components: core components and community-specific components. The NIEM's core components are further classified as either universal or common. Community-specific components are organized around functional lines of business, such as the maritime community, and are understood and managed by a specific community of interest, such as the GMCOI. Community-specific components can extend core components and must conform to the NIEM naming and design rules. Community specific components are organized to facilitate governance, and each has some measure of persistency. Communities traditionally include a cohesive group of data stewards who are subject matter experts (SMEs), have some level of authority within the communities they represent, and participate in the processes related to harmonizing conflicts and resolving data component ambiguities.

MIEM development began in 2006 to support collaborative tracking of vessels, people, and cargo. Also beginning in 2006, but as a separate initiative, the MDA DS COI was formed to define schemas for sharing sensor data, such as data received from Automatic Identification System (AIS) transponders. The MDA DS COI became a beta tester of the MIEM and has demonstrated successful modeling and sharing of that data. The approach for MDA data standards at the national level is to establish MIEM as the maritime community extension of NIEM.

UCore is an interagency initiative accomplishing a critical functional element of the National Information Sharing Strategy-establishing an information exchange specification and

Notional Representation of the MIEM as the Maritime Extension to the NIEM

implementation profile. This consists of a vocabulary of most commonly exchanged concepts, XML representation of the concepts, extension rules to allow tailoring to specific mission areas, security marking to permit controlled access, and a messaging framework to package and unpackage the content consistently. UCore Version 2.0 defines a small number of universally understandable concepts that are commonly shared and understood among all participating communities. Development of Version 2.0, has extended beyond the "Where" and "When" of Version 1.0 to include the "Who" and "What" components. During the alpha-testing phase, the UCore development team created and published an information exchange specification and coordinated approximately 20 risk reduction pilots conducted by various organizations in the DoD, Department of Homeland Security (DHS), Director of National Intelligence (DNI), and Department of Justice (DOJ).

The NIEM program has committed to ensuring that future versions of NIEM will be compatible with UCore. UCore has been designed to be interoperable with NIEM so that current NIEM-based systems can share information via UCore.

The MDA vocabulary will be an integration of MIEM, as the maritime community's extension to NIEM, and UCore products and services. This methodology will provide common processes and guidelines for metadata naming and design rules, extending the MDA core vocabulary, and registering metadata assets.

Standard Data Exchange Methodology

Current data exchange initiatives and methodologies employed by stakeholder organizations within and across the MDA community have created a web of terminology and data models that may not be interoperable. The standardized data exchange methodology for MDA must build upon and extend established methodologies, processes, and tools from MIEM, NIEM, and UCore successes. Recognizing the importance of using common information elements, the interagency community has begun to define a UCore model. While this model attempts to address the interoperability issue, it is necessary to ensure that this approach aligns with other efforts within and across the maritime community.

Success of the MDA mission relies on data exchange capabilities that are available, reliable, secure, and easy to find and use. Support mechanisms need to be in place to help users discover and access authoritative sources of data, understand the data, and select the items they need. Capabilities and resources need to be in place to support data and information sharing operations to include the tracking, reporting, and management of information exchange services and their associated infrastructure.

The standardized data exchange methodology must provide common processes and guidelines, and a consistent set of tools and services to enable the discovery of information across security and organizational communities, as well as to support the tagging and marking of data and services. The goals of this approach are to identify best practices for establishing standards for these basic core elements, increase the unity of effort at the strategic level, define cross-organizational standards for information exchange, recommend needed governance and support, and define common widely-accessible tools to support information exchange standards.

Information Assurance is a major area of focus for the MDA Architecture Management Hub. An acceptable level of trust is critical in enabling an information sharing environment involving multiple federal, state, tribal, and other sovereign nation organizations. However, the first step is agreeing to standards that all participating organizations consider trustworthy from an information assurance standpoint; i.e., the information systems can be trusted with the appropriate safeguards and countermeasures necessary to operate within defined levels of risk to organizational operations and assets, individuals, or other organizations, despite the possible environmental disruptions, human errors, and purposeful attacks that may occur. To achieve this level of trust, the IA processes within this net-centric environment must ensure a mutually agreed upon acceptable level of confidentiality, integrity, availability, and authentication of the information available. Therefore, the foundation of the MDA environment must have:

- The ability to securely exchange information, including classified and sensitive information, as well as intelligence and law enforcement sensitive data, across multiple security domains.
- An identity management solution that is shared, standards-based, and recognized and accepted by all MDA participants.
- Improved and standard security practices across the MDA environment.
- A risk management framework to ensure that information assurance security risks are addressed appropriately.

Cross-Domain and Multi-Level Security Solutions

There will be users within the MDA environment who may not have a security clearance but will need information derived from sources that may be highly classified and compartmentalized. Such information must first be sanitized and then must be able to move throughout the MDA environment. Likewise, personnel working on a classified network need to be able to access unclassified information in order to form a complete operating picture. Safely providing access to multiple levels of information and moving information between classification levels or organizational domains will require trusted solutions. The current Cross Domain Baseline for Distribution produced by the Unified Cross Domain Management Office (UCDMO) will be leveraged to achieve this requirement.

Identity Management Solution

Identity management provides the foundation that enables implementation of a need-to-share information paradigm; it is a critical enabler for the control of access to resources in a fashion that balances mission need with risk to resources. The Identity Management solution must enable federated services. There are three key components to such a solution: Identity Proofing when credentials are issued, Identity and Credential Authentication when the credentials are used, and Access Control to limit the user to appropriate access and actions.

Identity Proofing. Identity proofing is the keystone to the credibility, reliability, and accuracy of the overall identity management process, so that resultant credentials are bound directly to the actual identity of the individual requesting them when they are issued. The identity management solution must be able to support multiple requirements for identity proofing (e.g., man-to-man, man-to-machine, and machine-to-machine processes).

Identity and Credential Authentication. When an individual asserts an identity claim when accessing systems or services, an identity management service must authenticate that claim through the use of the credential issued to the individual. To achieve that goal, the credential must be authenticated. Credential authentication is a service that allows any entity in the enterprise to determine that a trusted credential has not been forged, has not expired, and has not been revoked or suspended. The authentication service must support scalable operations that remain accessible and robust in the face of cyber attacks. In implementing identity and credential authentication, we will draw upon the

lessons learned from ongoing efforts.

Access Control (Authorization). Critical in a net-centric cross-agency environment is access control–determining when a user is authorized to access information, systems, or services. All MDA users require immediate on-demand access to the range of products and services available within the MDA environment, regardless of the organization in which the product or service actually resides. Therefore the MDA data sharing environment must provide support for the unanticipated user–one not previously registered or enrolled with the organization providing services. An emerging means of providing this support in a net-centric environment is through Attribute-Based Access Control (ABAC). This approach allows decisions concerning access to information to be made based on organizational and enterprise attributes of the new user, rather than on prepared classification and permission assignments. ABAC in an interagency environment needs to be supported by robust and reliable identity management and attribute services. The federated identity management service must provide mutually trusted authentication of identity claims using credentials presented by the unanticipated user; the federated attribute management service must provide accurate attributes bound to an authenticated identity at the enterprise and local levels. This solution must consider not only the attributes currently available, but also the attributes that may be needed in the future. We will draw extensively on the lessons learned from the ABAC pilot that the MDA Data Sharing COI is currently conducting, and several other pilots being conducted throughout the DoD. We will also leverage work done by the Intelligence Community (IC) DoD Attributes and Authorization Tiger Team to provide a starting point for a CONOPS and standards.

Improved and Standard Security Practices across the MDA Environment

To share information among different organizations, there must be mutual trust in all participating organizations' information systems. To achieve this trust, all information systems must be certified, accredited, and maintained to an agreed upon set of standards. The standards for acceptable risk must be common across all participating organiza-

tions. Likewise, the risk determination by one organization for its data must be acceptable by any other organization whose data may reside on that organization's information systems.

Common Set of Standards for Certification and Accreditation (C&A) Activities. A common set of C&A standards and adherence to those standards are critical because these are the basis upon which trust in other organizations' information systems is established, thus allowing unfettered information access. This is especially true and critical if any participating organization uses an information system that will operate at a multi-level security (MLS) mode. The C&A Transformation Initiative, a joint DoD and DNI CIO effort to drastically streamline the C&A process for national security systems, and National Institute of Standards and Technology (NIST) Recommended Security Controls for Federal Information Systems (SP800-53), will be leveraged to achieve this requirement.

C&A Reciprocity. In a net-centric information-sharing environment, reciprocity for C&A activities across all participating organizations is critical. Once a common set of security standards is accepted by the participating organizations, the first step is reciprocity of the certifications with the ultimate goal of having reciprocity for both certifications and accreditations. Again, a joint DoD and DNI CIO effort to drastically streamline the C&A process for national security systems will be leveraged to achieve this requirement.

Controlled Unclassified Information (CUI). Since it is likely that much of the information in the MDA environment will qualify as CUI as defined by reference (l), it is necessary that participating organizations control and mark any CUI as

required by reference (l), so that it will be handled appropriately.
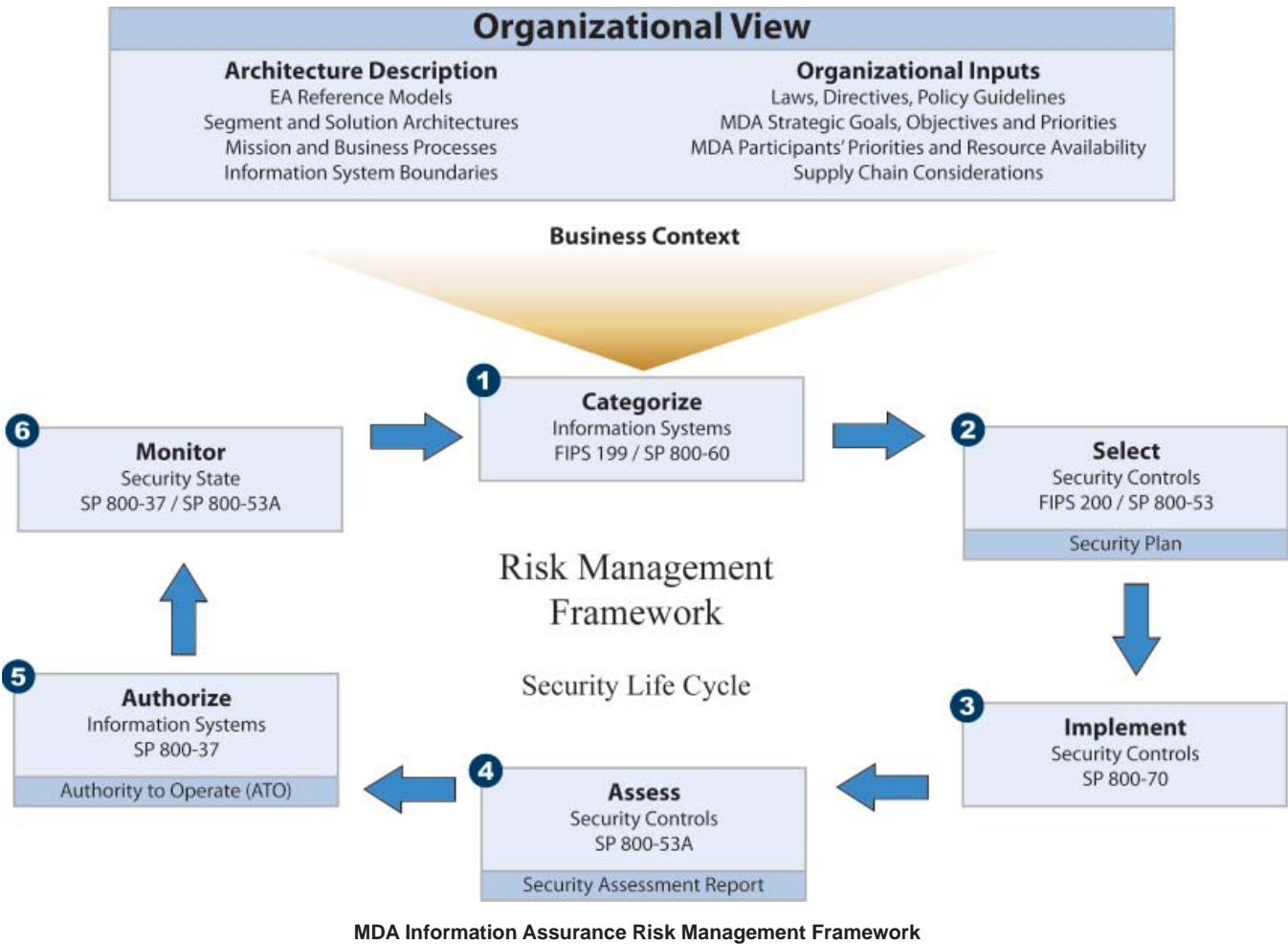
Risk Management Framework

The risk associated with information sharing among MDA participants must be continuously mitigated by employing a Risk Management Framework (RMF). The RMF provides GMCOI members with a disciplined, structured, flexible, extensible, and repeatable process for achieving agreed-upon degrees of trustworthiness for MDA information systems. The RMF, which operates within the context of the architecture development life cycle, can be applied to both new and legacy information systems that are part of the MDA environment. The RMF leverages well-defined information security standards and guidelines to facilitate the sharing of information and demonstrate compliance with the information security requirements. The plug-and-play nature of the RMF allows any potential MDA participant, e.g., federal, state, local, and tribal gov-ernments, private sector and international partners to use the framework. The RMF being developed by PM-ISE along with RMF initiatives being developed by NIST, CNSS and the IC will be leveraged to develop the MDA RMF.

The MDA RMF:
- Embodies the basic principles of information security – confidentiality, integrity, and availability – so that MDA participating organizations are assured that the information they provide will be protected adequately.
- Is integrated with the MDA Enterprise Architecture.
- Employs appropriate information security standards and guidance.
- The MDA RMF consists of the following steps, as illustrated by the figure below, with the NIST security standards and guidelines associated with each activity for risk management.

Step 1. Categorize the MDA information systems and information residing within the systems

MDA Information Assurance Risk Management Framework

based on the security category recommendations from the appropriate Information Security governance functions. This categorization must consider the potential impact of limiting access to the information, as well as potential impacts if the information is shared. The business context that consists of the applicable laws, directives, and policy guidelines as well as MDA strategic goals, objectives, and priorities must also be considered. The risks associated with each category must be identified and prioritized.

Step 2. Select, supplement, and document safeguards and countermeasures.

- Select an agreed upon set of safeguards and countermeasures for MDA information systems based on the prioritized technical risks, security categorizations, and recommendations from the MDA security governance functions.
- Supplement the agreed upon set of safeguards and countermeasures based on an assessment of the MDA participant's site specific risk conditions, including organizational-specific security requirements, specific and credible threat information, cost-benefit analyses, and special circumstances.
- Document the set of safeguards and countermeasures in the MDA information system security plan, including the rationale for any refinements and adjustments to the implemented set of safeguards and countermeasures based

on MDA participants' site-specific conditions.

Step 3. Implement the set of safeguards and countermeasures in the MDA information systems.

Step 4. Assess the safeguards and countermeasures using appropriate methods to determine the extent to which they are implemented correctly, operate as intended, and produce the desired outcome with respect to meeting the security requirements of the MDA information system. This step is key to demonstrating the degree of trustworthiness of the system, a critical input to the risk decision and maintenance of trust within the MDA environment. The assessment will be documented in the Security Assessment Report.

Step 5. Authorize the information system operation with the implemented safeguards and countermeasures based upon a determination that the risk to MDA participants' operations and assets, is acceptable. This step results in an Authority to Operate (ATO) for this particular MDA information system.

Step 6. Monitor and assess the documented and agreed upon set of safeguards and countermeasures in all MDA information systems on a continual basis. Document any changes to information systems, conduct security impact analyses of the associated changes, and report the security status of the information systems to appropriate MDA officials on a regular basis.

Resources dedicated to accomplishing the goal of a net-centric, information sharing environment as outlined in this document, will be applied toward two complementary efforts. First, resources are needed to design and develop the MDA enterprise architecture. Second, departments and agencies, guided by the architecture, will invest resources in a manner that will increase information sharing and lead to greater levels of MDA.

Designing an effective architecture to be utilized by the entire GMCOI will require an investment of time and expertise. To be successful, members of the GMCOI must be willing to contribute knowledgeable individuals to participate in the MDA Architecture Management Hub focus teams. These focus teams will set priorities and develop the standards and processes that will lead to a federated information sharing environment.

As the architecture is designed, budget authorities will gain a better understanding of the magnitude of the resource requirements necessary to implement capabilities to support MDA. The MDA enterprise architecture will act as guidance for investments which can contribute to MDA, and assist departments and agencies in their efforts to address the capability gaps highlighted in the Interagency Investment Strategy. The architecture will focus those efforts, help ensure interoperability, and prevent unnecessary redundancy. As segments of the MDA enterprise architecture are designed, members of the GMCOI can use the standards and processes developed to inform their acquisition plans. Design of the architecture will leverage existing and emergent infrastructure, systems, services, and other initiatives. Therefore, much of the cost will be borne by those efforts.

Summary

As the lead for the MDA Architecture Management Hub, the DON CIO will follow the approach outlined in this document to design an actionable MDA enterprise architecture that can guide implementation efforts to achieve a secure, collaborative information sharing environment for the GMCOI. This architecture will build on the work of other organizations and draw upon the expertise of individuals from those organizations. Working within the governance structure created by the MDA CONOPS, the Architecture Management Hub will develop a set of complementary architectural models. These models will constitute the core of an as-is and to-be MDA Enterprise Architecture. They will serve as the basis for development of an architecture migration and implementation plan.
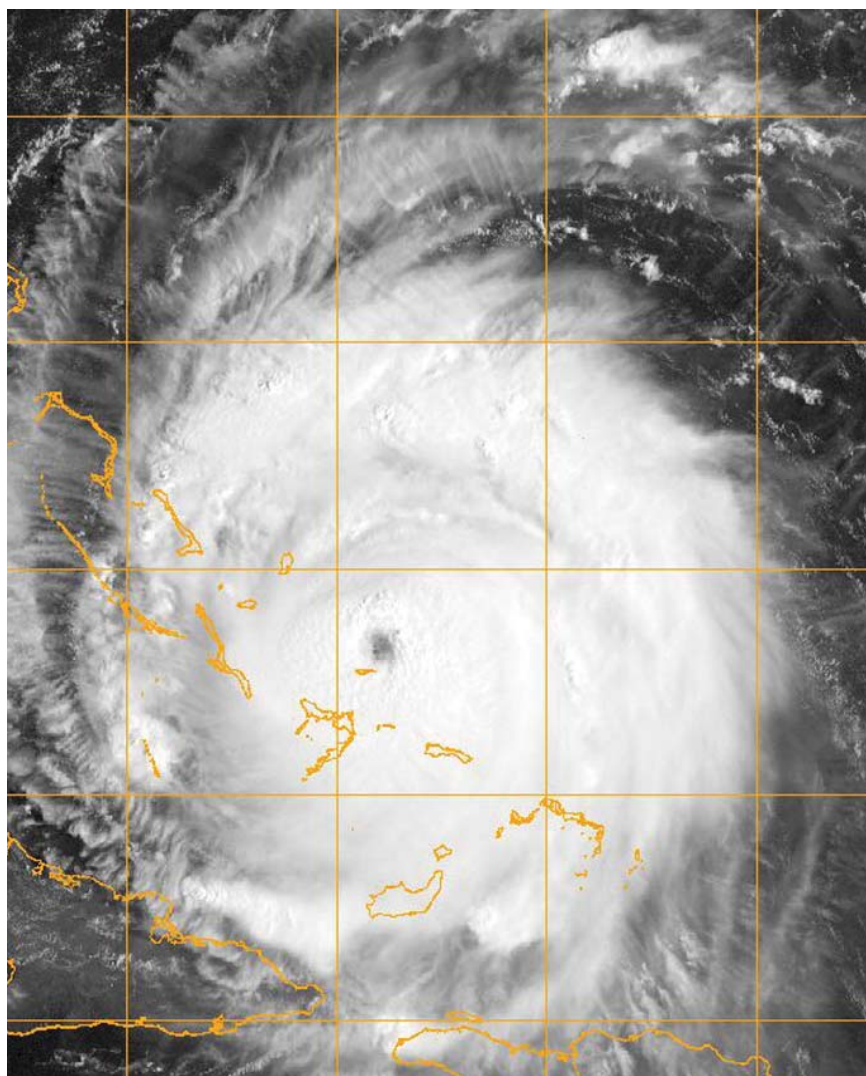
By following this document's approach to establishing and implementing data standards, the resulting architecture will provide data and information exchange standards that permit organizations to publish information for use by authorized users. The MDA Architecture Management Hub will also recommend standard solutions for sharing information across security domains, when authorized and appropriate, and for controlling information access.

Implementation of this plan will follow an iterative process, beginning with agencies and departments within the Federal Government and adding products and services over time. As soon as this process is in place and functioning, representative organizations from state, local, and tribal governments, as well as appropriate representatives from the private sector and international organizations will be invited to participate. The work of the Architecture Management Hub will benefit all members of the GMCOI, and increased participation will have exponential rewards for all. Members of the GMCOI from outside the Federal Government must be involved early in the process to promote greater efficiencies and minimize the risk of incompatible solutions.

The work of the MDA Architecture Management Hub will extend well beyond the GMCOI. The information sharing standards and methods developed for MDA will have application throughout the Federal Government and beyond. The processes and methodologies developed by this effort can benefit COIs and organizations facing similar information challenges.

Guidance for MDA information sharing is derived from the following documents:

A. National Plan to Achieve Maritime Domain Awareness for the National Strategy for Maritime Security, October 2005

B. Global Maritime Intelligence Integration Plan for the National Strategy for Maritime Security, October 2005

C. National Concept of Operations for Maritime Domain Awareness, December 2007

D. National Maritime Domain Awareness Interagency Investment Strategy, May 2007

E. MDA Interagency Requirements Analysis (IARA)

F. National MDA Study Inter-agency Needs Analysis (IANA), December 21, 2006

G. MDA Interagency Capabilities Document, Version 2.0.3, 31 January 2007 (IACD)

H. MDA Interagency Core Architecture Document (IACA), Draft Version 1.2, February 08, 2007

I. National Strategy for Information Sharing, October 2007

J. Information Sharing Environment Enterprise Architecture Framework, v.2.0 September 2008

K. Executive Order 13388, Further Strengthening the Sharing of Terrorism Information to Protect Americans, October 25, 2005

L. Presidential Memorandum, Subj: Designation and Sharing of Controlled Unclassified Information (CUI), May 9, 2008

M. NIEM Program Management Office, Introduction to the National Information Exchange Model (NIEM), version 0.3, February 12, 2007 (available at http://www.niem.gov/files/NIEM_Introduction.pdf)

N. United States Intelligence Community Information Sharing Strategy, February 22, 2008

O. Department of Homeland Security Information Sharing Strategy, April 18 2008

P. DoD Directive 2005.02E Maritime Domain Awareness (MDA) in the Department of Defense

Q. DoD Information Sharing Strategy, May 4, 2007

R. DoD Directive 8500.01E, Information Assurance (IA), October 24, 2002

S. DoD Net-Centric Data Strategy, May 9, 2003

T. DoD Directive 8320.02, Data Sharing in a Net-Centric Department of Defense, December 2, 2004.

U. FIPS PUB 201-1: Personal Identity Verification (PIV) of Federal Employees and Contractors

V. National Maritime Intelligence Center (NMIC) Integrated Maritime Intelligence Architecture (IMA) Transformation Strategy, Release Version 1.1 , 01 March 2007

Acronyms

Acronym	Full Text
ABAC	Attribute Based Access Control
AIS	Automatic Identification System
C&A	Certification and Accreditation
CES	Core Enterprise Services
CBP	Customs and Border Protection
COI	Community of Interest
CONOPS	Concept of Operations
CNSS	Committee on National Security Systems
CUI	Controlled Unclassified Information
DHS	Department of Homeland Security
DNI	Director of National Intelligence
DoD	Department of Defense
DoDAF	DoD Architecture Framework
DOJ	Department on Justice
DON	Department of the Navy
DON CIO	Department of the Navy Chief Information Officer
DOT	Department of Transportaion
DS COI	Data Sharing Community of Interest
FEA	Federal Enterprise Architecture
FSAM	Federal Segment Architecture Methodology
GMAII	Global Maritime and Air Intelligence Integration
GMCOI	Global Maritime Community of Interest

Acronym	Full Text
GMSA	Global Maritime Situation Awareness
IA	Information Assurance
IACA	Interagency Core Architecture Document
IC	Intelligence Community
IMA	Integrated Maritime Intelligence Architecture
IOOS	Integrated Ocean Observing System
ISE	Information Sharing Environment
ISE EAF	Information Sharing Environment Enterprise Architecture Framework
ISSC	Information Sharing Sub Committee
IT	Information Technology
MDA	Maritime Domain Awareness
MIEM	Maritime Information Exchange Model
MLS	Multi Level Security
NCES	Net-Centric Enterprise Services
NIEM	National Information Exchange Model
NIST	National Institute of Standards and Technology
NOAA	National Oceanographic and Atmospheric Administration
PII	Personally Identifiable Information
SME	Subject Matter Experts
SOA	Service Oriented Architecture
Ucore	Universal Core

Change History

Version	Publication Date	Description of Change
1.0	10/2008	Initial DON CIO Release
1.1	01/2009	Incorporate Interagency Action officer Comments
1.2	01/2009	Incorporated Interagency Flag/General Officer and SES Comments

This page Left Intentional Blank