DoD 8320.02-G

Guidance for Implementing Net-Centric Data Sharing

April 12, 2006
Assistant Secretary of Defense for
Networks and Information Integration/
Department of Defense Chief Information Officer

DEPARTMENT OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

CHIEF INFORMATION OFFICER

April 12, 2006

FOREWORD

This Guide is issued under the authority of Department of Defense (DoD) Directive 8320.2, "Data Sharing in a Net-Centric Department of Defense," December 2, 2004 (Reference (a)). It provides implementation guidance for the community-based transformation of existing and planned information technology (IT) capabilities across the Department of Defense (DoD) in support of Department-wide net-centric operations.

This Guide applies to the Office of the Secretary of Defense, Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities within the DoD (hereafter referred to collectively as the "DoD Components").

This Guide is effective immediately and is available for use by all the DoD Components.

Send recommended changes to this Guide to the following address:

Director
Information Management Directorate Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD (NII)/DoD CIO)
6000 Defense Pentagon
Washington, DC 20301-6000

The DoD Components, other Federal Agencies, and the public may download this Guide from the DoD Metadata Registry, http://metadata.dod.mil, or from the Washington Headquarters Services web page at http://www.dtic.mil/whs/directives.

Assistant Secretary of Defense for Networks and Information Integration/
DoD Chief Information Officer

TABLE OF CONTENTS

TABLES

REFERENCES

(a) DoD Directive 8320.2, “Data Sharing in a Net-Centric Department of Defense,” December 2, 2004
(b) DoD Chief Information Officer Memorandum “DoD Net-Centric Data Strategy,” May 9, 2003[1]
(c) DoD Discovery Metadata Specification (DDMS)[2]
(d) DoD Directive 8500.1, "Information Assurance," Oct 24, 2002
(e) DoD Directive 8115.01, “Information Technology Portfolio Management,” October 10, 2005
(f) DoD Directive 4630.5, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” May 5, 2004

[1] Available at the following website: http://www.defenselink.mil/nii/org/cio/doc/Net-Centric-Data-Strategy-2003-05-092.pdf.
[2] Available at the following website: http://diides.ncr.disa.mil/mdreg/user/DDMS.cfm.

DL1. DEFINITIONS

TERMS AND DEFINITIONS

DL1.1.1. Data Producer. Refers to a program, organization, or even a person that controls, manufactures, and/or maintains data assets within the Department.

DL1.1.2. Schema. A diagrammatic representation, an outline, or a model. In relation to data management, a schema can represent any generic model or structure that deals with the organization, format, structure, or relationship of data. Some examples of schemas are (1) a database table and relational structure, (2) a document type definition (DTD), (3) a data structure used to pass information between systems, and (4) an XML schema document (XSD) that represents a data structure and related information encoded as XML. Schemas typically do not contain information specific to a particular instance of data.

DL1.1.3. Semantic metadata. Information about a data asset that describes or identifies characteristics about that asset that convey meaning or context (e.g., descriptions, vocabularies, taxonomies).

DL1.1.3.1. Vocabulary. Represents agreements on the terms and definitions common to the COI, including data dictionaries. For example, one COI might define the term "tank" to mean a pressurized vessel, whereas another might define "tank" to mean a tracked vehicle. Both definitions are acceptable, but the user must understand these definitions, and their context, to properly use the data.

DL1.1.3.2. Taxonomy. Provides categorizations of related terms. In doing so, they make use of "class/subclass" relationships (i.e., they are hierarchical in conveying the relationships between categories). Taxonomies are important to ensuring that searches of discovery metadata and content are targeted. An example taxonomy of the various types of ISR data in several dimensions might be as follows:

INT Type: HUMINT, SIGINT, ELINT, MASINT...
Source Type: Human, Airborne, Space-based, ...
Source Level: National source, tactical source, open source...
Trust Level: Unevaluated, validated,…..
Collection Purpose: Force protection, tactical, strategic, ….

DL1.1.3.3. Ontology. An explicit specification of how to represent the objects and concepts that exist in some area of interest and of the relationships that pertain among them.

DL1.1.4. Website. A collection of web pages, that is, HTML/XHTML documents accessible via Hypertext Transfer Protocol (HTTP) on the Internet, an intranet, or another network. The pages of a website can be accessed from a common root uniform resource locator (URL) using common web browsers. The URLs of the pages organize them into a hierarchy, although the hyperlinks between them control how the reader perceives the overall structure and how traffic flows between the different parts of the site.

AL1. ACRONYMS

COI. Community of Interest

CIO. Chief Information Officer

DDMS. DoD Discovery Metadata Specification

DISR. DoD Information Technology Standards Registry

HTML. Hypertext Markup Language

POAM. Plan of Action and Milestones

POC. Point of Contact

PoR. Program of Record

ROI. Return on Investment

UDDI. Universal Description, Discovery and Integration Protocol

XML. Extensible Markup Language

C1. CHAPTER 1

INTRODUCTION

C1.1. PURPOSE

This "Guidance for Implementing Net-Centric Data Sharing" document is designed to complement Reference (a). Reference (a) codifies the DoD Chief Information Officer (CIO) Memorandum (Reference (b)), which describes the Department's official vision for data and information sharing in a net-centric environment through collaborative forums known as communities of interest (COIs). The goal of this Guide is to provide a set of activities that members of COIs and associated leadership can use to implement the key policies of Reference (a) and ultimately increase mission effectiveness across the Department of Defense. The activities presented in this Guide may not apply to all COIs and should be tailored as necessary.

C1.2. AUDIENCE

This Guide is intended primarily for COI members. These members come from across the Department of Defense and include DoD Component representatives such as operators, subject matter experts, and representatives from programs and systems (e.g., capability developers). In addition, this Guide provides information to enable DoD Component CIO and Mission Area and subportfolio leadership throughout the Department of Defense to understand how COIs can implement the key policies of Reference (a).

C1.3. DOCUMENT OVERVIEW

C1.3.1. This Guide is organized in four chapters. Chapter 1 describes the purpose of the document, its intended audience, and the document structure. Chapter 2 provides an overview of COIs and the roles and responsibilities of the various organizational entities relative to COIs. Chapter 3 provides a set of activities for COI formation and execution, along with suggested approaches for governing and managing the development of new data sharing capabilities. Chapter 4 provides detailed guidance for implementing the key policies of Reference (a), organized by implementation areas composed of specific activities. Note that this Guide uses the terms information sharing and data sharing interchangeably.

C1.3.2. Readers new to COIs or those in the process of forming a COI should consult Chapters 2 and 3 for guidance on establishing a COI, setting up governance structures, defining data sharing mission, etc. Established COIs or groups working on building new information sharing capabilities can read Chapter 4 for specific activities for implementing data sharing, but will benefit from reading Chapters 2 and 3 for a comparative approach to establishing a COI.

C1.3.3. The activities described in Chapters 3 and 4 may also include, where appropriate, "Enterprise Considerations" and "Technical Guidance." Enterprise Considerations tie the COI activities back to Department of Defense goals, while Technical Guidance provides additional technical information and references related to an activity. "Forward Planning" activities are also provided for COIs to consider implementing or addressing at a later stage (e.g., operations and maintenance activities).

C1.3.4. Where this Guide describes activities that can be undertaken by a COI, the intent is for COI members to execute these activities. However, activities may not require full participation by all COI members. For example, subject matter experts may be primarily engaged in defining semantics whereas capability developers may be primarily engaged in defining and implementing services to make data accessible. This Guide also recognizes that some activities, such as implementation of many of the COI agreements, will require planning and budgeting by DoD Components, as well as influence by Mission Area leads.

C1.3.5. This Guide is a living document and will continue to be updated with best practices and lessons learned as the Department of Defense gains experience implementing data sharing through COIs.

C2. CHAPTER 2

THE ROLES, RESPONSIBILITIES, AND RELATIONSHIPS OF THE COI IN INFORMATION SHARING

C2.1. KEY COI ATTRIBUTES

C2.1.1. Reference (b) defines the COI as "a collaborative group of users who must exchange information in pursuit of their shared goals, interests, missions, or business processes and who therefore must have shared vocabulary for the information they exchange." COIs are organizing constructs created to assist in implementing net-centric information sharing. Their members are responsible for making information visible, accessible, understandable, and promoting trust – all of which contribute to the data interoperability necessary for effective information sharing. This chapter describes the roles, responsibilities, and relationships of COIs in information sharing.

C2.1.2. The focus for COIs is to gain semantic and structural agreement on shared information. For COIs to be effective, their scope—that is, the sphere of their information sharing agreements—should be as narrow as reasonable given their mission. Although the Department of Defense or a Military Department might be considered a collaborative group of users who have a shared mission, and thus a COI, achieving a shared vocabulary across the entire Department of Defense or even across a Military Department has proved to be very difficult to achieve due to the scope and magnitude of the information sharing problem space. COIs represent a mechanism for decomposing the Department of Defense's information sharing problem space into manageable parts that can be addressed by those closest to the individual parts.

C2.1.3. COIs may be guided by the Department of Defense's strategic goals, existing policy, and doctrine, or COIs may form on an ad hoc basis to address a data sharing problem among known stakeholders. While Component-specific COIs may exist, COIs are most likely to be functional or joint entities that cross organizational boundaries. An example of a COI might be a meteorology COI or a joint task force. COIs should include producers and consumers of data, as well as developers of systems and applications.

C2.1.4. Although COIs may vary, the key attributes presented in Table C2.T1. should be applicable for the majority of COIs across the Department of Defense.

Table C2.T1. Key COI Attributes

• Formed to meet a specific data sharing mission or fulfill a task
• Composed of stakeholders cooperating on behalf of various organizations, with emphasis on cross-Component activities
• Members committed to actively sharing information in relation to their mission and/or task objectives
• Recognize potential for authorized but unanticipated users and therefore, strive to make their data visible, accessible, and understandable to those inside and outside their community.

C2.1.5. As a COI evolves, its membership, mission, and related tasks also evolve. Some expedient, or temporary, COIs will form to accomplish a specific mission based on improved information sharing and disband once the mission is accomplished. These COIs will have relatively short life spans. Other COIs may continue to operate on the basis of a continuing mission need, otherwise known as institutional COIs. While the Department of Defense transitions to an improved information sharing culture and environment, we expect both expedient and institutional forms of COIs to exist. Regardless of the nature of the COI, the key attributes as listed in Table C2.T1., and the primary responsibilities of the members shown in Table C2.T2. are equally applicable. Where COIs may differ is in the execution of the activities described in Chapters 3 and 4 of this Guide to achieve their data sharing mission and satisfy their primary responsibilities.

Table C2.T2. Primary Responsibilities of COIs

- Identify data assets and information sharing capabilities, both operational and developmental, that should conform to the data strategy goals of Reference (b).
- Identify approaches to enable those data assets and information sharing capabilities to satisfy data strategy goals and to measure the value to consumers of shared data.
- Develop and maintain semantic and structural agreements to ensure that data assets can be understood and used effectively by COI members and unanticipated users.
- Register appropriate metadata artifacts for use by the COI members and others.
- Extend the DoD Discovery Metadata Specification (DDMS) (Reference (c)) as required to ensure that COI-specific discovery metadata is understandable for enterprise searches.
- Partner with a governing authority, as appropriate, to ensure that COI recommendations are adopted and implemented through programs, processes, systems and organizations.

C2.1.6. COI members may come from any area of the Department of Defense. In specific cases, members of COIs may come from outside the DoD community (e.g., National Intelligence Community, allies, industry) to provide subject matter expertise. COI membership consists of DoD Component representatives, program managers, system owners, developers, data consumers, DoD Component leadership, portfolio managers, and others, all of whom can contribute in different ways to COI activities. This Guide refers to COI members by the role that they play within the COI. Table C2.T1. describes these COI roles based on how they interact with the COI and other organizational entities.

Table C2.T3. Summary Descriptions of COI Roles

ROLE	DESCRIPTION
COI Governing Authority	Individual or organization that will review and adjudicate COI conflicts and push for DoD Component implementation and support of COI data sharing agreements. The appropriate governance forums and authorities may already exist and should be leveraged where possible. This role is typically filled by the Mission Area lead, but in the initial stages of operationalizing portfolio management, may also be a Combatant Command or Functional Support Agency (e.g., DLA). The COI governing authority acts as an external champion with authority and cross-COI visibility to affect change. Responsibilities: • Identify information sharing problems and COI missions • Review and adjudicate resolution of discrepancies across COIs

	• Promote and endorse COI activities and implement agreements through the Joint Capabilities Integration and Development System, Acquisition, and Planning, Programming, Budgeting, and Execution process • Promote COI support to DoD Components • Review COI plan of action and milestones (POAM) status and success measures
COI Lead	An individual from a specific DoD Component who has been tasked with managing the COI. Generally, the organization leading the COI activity has committed to driving the COI to a data sharing solution and will advocate that data sharing agreements be implemented within DoD Component plans, programs, and budgets. The COI lead helps address internal COI conflicts and issues, keeping the COI on track. The COI lead role may be established on a shared or rotating basis, and should be filled by a functional expert, rather than an IT specialist. Responsibilities: • Ensure that appropriate stakeholders participate in COIs via COI working groups, and appropriate representatives participate via the governing authority • Lead the COI, including developing and tracking POAMs • Act as a primary point of contact (POC) for the COI • Promote policies and practices for data sharing and participating in cross-Component COIs • Identify mission-specific success criteria for the COI
COI Stakeholders	Organizations or personnel who have an interest in the outcome of the COI effort. These may not be active participants in the COI, but will likely use and/or benefit from the capability, such as data consumers. COI stakeholders are those who stand to benefit, and those whose processes and/or systems will change, as a result of COI activity. Responsibilities: • Promote policies across DoD Components in terms of practices and standards in the implementation areas, including those for data tagging, data access services, and registration of metadata artifacts • Promote the reuse of data access services within programs and systems • Track DoD Component implementation of Reference (a) through COI activities • Ensure operator/end-user views and needs are represented in COI semantic and structural agreements, contribute to COI requirements gathering processes, and provide feedback on COI-defined information sharing capabilities
Capability Developers	Personnel or organizations responsible for serving as the technical representative and implementing the data sharing agreements (e.g., data access services), and applying technical approaches (e.g., tools for associating discovery metadata with data assets). Capability developers are the critical COI participants that turn COI agreements and requirements into live information sharing capabilities. Responsibilities: • Identify technical requirements for supporting information sharing capabilities (e.g., common tagging tools) and recommend the necessary programming and budgeting changes for supporting them efficiently • Participate in COI working groups, particularly as they relate to architectures, standards, and technical specifications

	• Identify implementation alternatives, including common or reusable services or technical capabilities • Identify technical impacts of COI agreements, for example the impact of a data access service on system performance to critical users • Implement and maintain agreed-upon capabilities • Ensure operator/end-user views and needs are represented in COI semantic and structural agreements
Data Producers	A program, organization, or person that controls, creates, and/or maintains data assets within the Department. These are typically the DoD Component program managers and system owners who provide the resources to implement data sharing agreements within their programs.
Subject Matter Experts	Individuals who represent specific operators and possess knowledge of their business processes. Responsibilities: • Ensure operator/end-user views and needs are represented in COI semantic and structural agreements • Advise the governing authority on subject matter priorities • Promote use of COIs to solve data sharing problems and advocate for implementation of COI agreements • Assist in the identification of mission-specific value measures for COI success

C2.1.7. COIs must observe all existing policy and guidance with respect to information assurance, protection and security according to DoD Directive 8500.1 (Reference (d)). This Guide does not provide COIs the authority to share information in any way that is prohibited by law, policy, or security classification.

C2.2. THE COI'S RELATIONSHIP TO THE ENTERPRISE

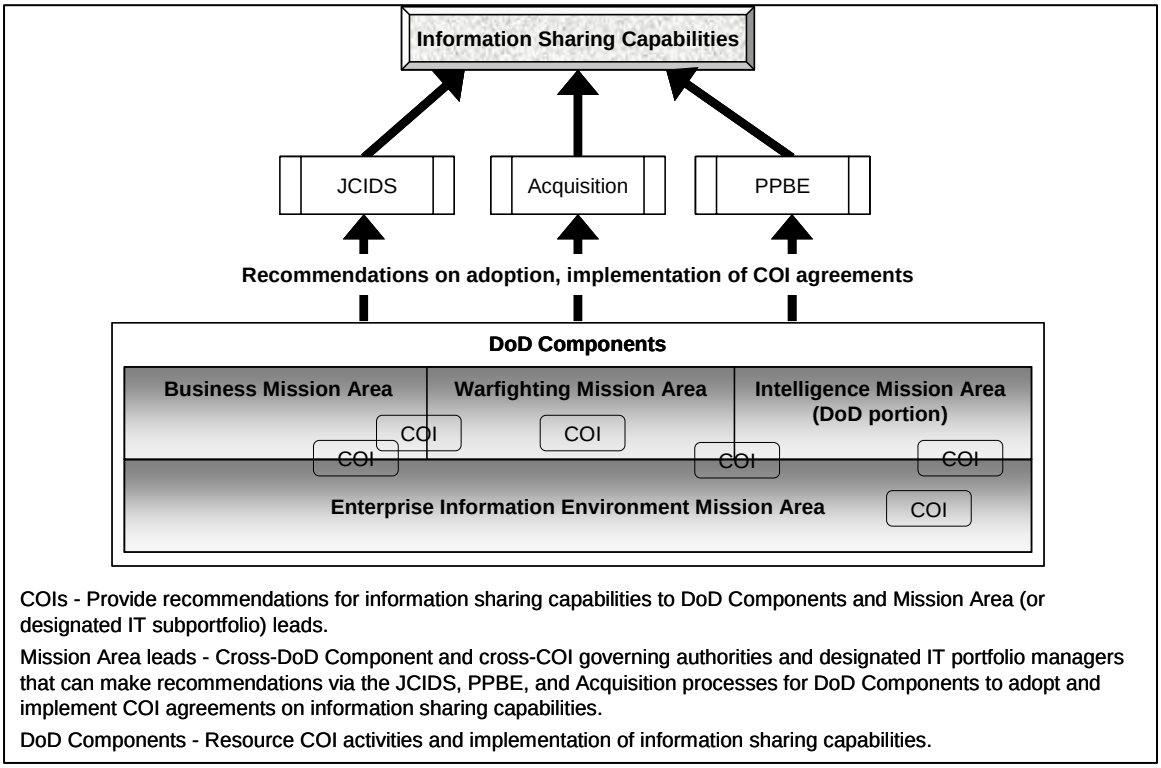
C2.2.1. COIs are typically cross-DoD Component groups that come together to address a specific information sharing mission or challenge that the COI can solve by exposing and sharing data. COI solutions or agreements will typically involve programs, organizations, or data assets belonging to multiple DoD Components, thus, many entities within the Department of Defense have a role in the success of information sharing capabilities identified by COIs.

C2.2.2. COIs will identify data sharing capabilities that DoD Components should consider implementing to solve mission problems. As a result, DoD Components plan, program, and budget to resource multiple COI agreements that the DoD Component must consider along with other DoD Component priorities.

C2.2.3. Mission Areas, as defined in the evolving DoD IT portfolio management construct under DoD Directive 8115.01 (Reference (e)), are cross-DoD Component portfolios of related IT investments. By definition, any Mission Area will span many or all DoD Components within the Department of Defense. Mission Area leads (or their respective subportfolio managers such as Domains, core business areas, or capability areas) have responsibility for looking across multiple DoD Component IT investment plans and budgets to identify the best value for the Enterprise.

C2.2.4. COIs make recommendations to Mission Area leads. Mission Area leads then rationalize and balance any conflicting COI recommendations. For example, COI members might agree that a particular program should make its data accessible via a web service using a particular common data schema. Mission Area leads can review and recommend which COI agreements should be implemented when conflicts or constraints arise. Mission Area recommendations are provided as input to the major decision processes that influence DoD Component plans, programs, and budgets. For example, a recommendation might have one DoD Component plan and budget for a data sharing capability while other DoD Components plan to reuse that same capability rather than expending resources to re-create it. This relationship between COIs, DoD Components, and Mission Areas to promote the implementation of information sharing capabilities is illustrated in Figure C2.F1.

Figure C2.F1. Relationship Between COIs and the Enterprise



COIs - Provide recommendations for information sharing capabilities to DoD Components and Mission Area (or designated IT subportfolio) leads.

Mission Area leads - Cross-DoD Component and cross-COI governing authorities and designated IT portfolio managers that can make recommendations via the JCIDS, PPBE, and Acquisition processes for DoD Components to adopt and implement COI agreements on information sharing capabilities.

DoD Components - Resource COI activities and implementation of information sharing capabilities.

C2.2.5. While the Department of Defense is in the early stages of establishing IT portfolio management, it is important for COIs to identify an appropriate cross-DoD Component board or body that can adjudicate disagreements on data semantics and implementation approaches that conflict across COIs. Combatant Commands and functional support agencies, as identified in Table C2.T1, may serve as viable boards or bodies for cross-COI conflict resolution and sponsorship, as well as being advocates for COI agreements in DoD Component plans, programs, and budgets. COIs should leverage existing governance constructs, forums, and working groups whenever possible to achieve their information sharing goals.

C3. CHAPTER 3

COI FORMATION AND EXECUTION

C3.1. CHAPTER OVERVIEW

C3.1.1. This chapter provides a set of activities to help guide the establishment, evolution, and operations of a COI, as well as the fielding of real information sharing capabilities. Readers new to COIs, in the process of organizing a COI, or belonging to a newly-formed COI should consult this chapter. Members of short-term COIs or participants who are already familiar with the activities involved in organizing a community may wish to move on to Chapter 4 which describes implementation of Reference (a).

C3.1.2. COIs may take various forms and are not intended to be "one size fits all." These groups can differ in how they operate, the timelines for their actions, the duration of their existence, how they are governed, and whether or not they demonstrate information sharing capabilities through pilot activities before operational use. As such, COIs should determine what activities, and associated levels of effort, are necessary to ensure sufficient governance and management of the COI.

C3.2. ESTABLISH AND EVOLVE A COI

C3.2.1. Activity Area Overview

C3.2.1.1. The establish and evolve activity area focuses on identifying the purpose for a community, identifying the community's needs, and establishing a COI to work toward meeting those needs. The initial step in forming a COI is to identify a potential need for such a group, the mission, and potential membership. In addition, before establishing a new COI, potential members should identify other organizations and/or COIs that may be addressing the same or similar problem area.

C3.2.1.2. If a similar COI exists and there is considerable semantic overlap in the identified problem area, potential members should reach out to the existing COI to leverage its work and investigate opportunities for collaboration. Assuming that a new COI is required, the process of establishing a new COI will involve the activities below. This section describes activities that aid implementation of the COIs referenced in section 4.7 of Reference (a).

C3.2.2. Implementation Activities

C3.2.2.1. Identify mission, members, and desired information sharing capabilities. The initial membership of a COI will come together around a common information sharing mission that can be addressed as a community. The COI's mission can be formally articulated through a mission statement or charter if the members consider this appropriate. COIs can refer to guidance provided in Chapter 2 to identify additional members. The COI should outline the purpose of the community and the

scope of its activities, identifying key capabilities that enable the COI to accomplish its mission. Executing these steps ensures that COI agreements reflect end-user needs, that those agreements are technically viable to implement, and that they have the ownership and buy-in necessary to promote changes in operational programs and systems.

C3.2.2.2. Identify related COIs. Communities should use the COI Directory[1] to identify related efforts for coordination of governance forums and sharing experiences. This directory maintains a listing of all DoD COIs that register, and provides visibility into their activities. Identification of other COIs can both inform the decision to establish a new COI and identify information sharing possibilities once a new COI has been established.

C3.2.2.3. Prioritize information sharing capabilities. COIs should prioritize key capabilities to focus their efforts based on the potential mission value and feasibility of implementation. In identifying such information sharing capabilities, COIs should consider use of both new and legacy systems. Prioritization should help keep the scope of any COI-identified information sharing capabilities focused and facilitate the implementation of pilots, or initial operational capabilities, as quickly as possible. This enables the COI to contribute to the delivery of real value quickly while providing lessons learned before additional capabilities are developed.

C3.2.2.4. Advertise the COI. To ensure that DoD users can discover the existence and mission of a COI and have the opportunity to participate, a member of the COI should register the COI in the COI Directory. To register, COIs should provide their name, POC, mission, status, COI lead, and proposed governing authority.

C3.2.3. Forward Planning

C3.2.3.1. Identify measures of success. COIs should define COI-specific success measures and measure progress against those criteria. Some measures will be mission specific. For example, success might be defined as reducing the time required to plan strikes as a result of having information available. Other measures of success might be non-mission specific. Non-mission specific measures can provide valuable insight enabling others in the Enterprise to assess data sharing approaches. For example, a COI could measure time saved in fielding new information sharing capabilities as a result of reusing existing data assets rather than re-creating data. Instituting measures of success helps ensure that the Enterprise continues to invest in those opportunities that provide value to the Enterprise.

C3.2.3.2. Continually gather user feedback. COI members should strive to meet user needs, measure the value achieved through information sharing, and work with stakeholders to identify near-term information sharing capabilities. As the COI evolves, so will stakeholder priorities and needs. Periodically, members should reassess activities to ensure that the COI is continuing to provide value and that it continues to address the COI's mission with needed capabilities. This reassessment would include its support for

[1] Available at the following website: https://gesportal.dod.mil/sites/coidirectory/default.aspx

net-centric information sharing across the Department of Defense. COI members should assess metric results to determine when the COI has achieved its mission and should disband or turn over operations to continuing organizations.

C3.3. COI MANAGEMENT AND GOVERNANCE

C3.3.1. Activity Area Overview

C3.3.1.1. The COI management and governance activity area focuses on identifying a governing body, communicating with stakeholders, and providing leadership and direction to the COI. COI management and governance activities are integral to ensuring that COIs achieve their mission. Although these activities will be tailored to the individual COI's mission and the membership, there are basic issues that a COI should address. These issues include, but are not limited to, information flow, issue adjudication, prioritization of COI activities, quality assurance, recommendations to portfolio managers, and configuration management (CM) of COI products. COI management is responsible for establishing governance processes and structures appropriate to the COI. This effort includes leveraging existing processes and structures where possible and appropriate.

C3.3.1.2. A COI's ability to facilitate cross-Component portfolio management for IT investments is essential for effective COI management. In IT portfolio management, designated Mission Area and subportfolio leads conduct reviews of DoD Component plans and budgets and ensure alignment and efficient use of resources that may advance COI-defined capabilities. As an example, the Intelligence Surveillance Reconnaissance (ISR) COI establishes the expectation that the DoD Components will support inter-Domain/inter-Component information sharing among the Distributed Common Ground System (DCGS) Family of Systems (FoS) program services. The ISR COI provides this direction through the prescribed use of common, shared, or federated information sharing services; specific data implementation strategies and tools, and COI specific agreement on access controls and security mechanisms. For subsequent portfolio reviews, the portfolio manager or identified COI governing authority bases the review on the ISR COI's guidance and works with the DoD Components to validate that each of the DCGS FoS programs are aligned and each has sufficient funding to effectively implement the COI-defined information sharing services and capabilities.

C3.3.2. Implementation Activities

C3.3.2.1. Identify governing authority. COIs should align themselves with an existing governing authority, such as a Mission Area lead, to enable the COI to impact the necessary related systems, programs, and data holdings. Mission Area leads may direct COIs to align themselves with a particular governing authority. Ideally, this governing authority should have flag or general officer level authority, without which the COI might lack the decision-making and resource authority to realize its information sharing goals. The governing authority should be in a position to influence agreements and to help address issues that affect multiple DoD Components.

C3.3.2.2. Select a COI lead. The COI lead is the POC and action officer for COI activities. This role differs from that of the governing authority in that the COI lead is responsible for the day-to-day functioning of the COI but should be in a position to influence agreements and to help address issues that affect multiple DoD Components. The COI lead interfaces with the COI governing authority to report status, resolve issues, promote COI agreements, and to make recommendations on Component's plans and schedules. Other responsibilities include leading regular meetings; establishing working groups, as needed; identifying other potential members; acting as a liaison to the portfolio manager or other governing authority; coordinating with the relevant program or system managers; collaborating with other COIs to reuse metadata artifacts; and helping to mitigate any conflict within the COI.

C3.3.2.3. Establish COI-specific governance processes. COIs should develop internal governance processes or leverage existing processes appropriate to the scope and mission of the COI. These activities include appropriate review and adjudication of issues and establishment of Memorandums of Agreement (MOAs) or Memorandums of Understanding (MOUs) as a set of working agreements among participants and their respective organizations. In addition, COI governance processes should enable the establishment of working groups, as needed, to address COI focus areas. For example, the COI might task a data working group with developing COI categorization schemes, thesauri, vocabularies, and taxonomies. COIs should ensure that their working groups operate with defined timelines, focus area(s), and deliverables.

C3.3.2.4. Clarify relationships between groups involved in the COI. Although COI members share a mission, establishing a clear understanding of information sharing relationships among members rather than assuming that such an understanding already exists will help shape COI responsibilities and direction.

C3.3.2.5. Share COI information with all stakeholders. An important aspect of management and governance is transparency of information. COI members must communicate with one another and the governing authority, as well as with their respective organizations. To this end, COIs should track and publicize their activities, schedules, actions, and progress. In addition, COIs should provide stakeholders with the results of specific metrics and measurements (i.e. assessment of performance against metrics) including progress in implementing new information sharing capabilities and progress towards implementing policy according to Reference (a). This process includes involving stakeholders in the review of documents and specifications developed by the COI and providing the community with mechanisms for user feedback.

C3.3.2.6. Assess reusability of other resources. Using the DoD Metadata Registry,[2] communities should identify opportunities for semantic and structural metadata reuse. COIs should also consult other COIs for opportunities to capitalize on operational data access services that can enrich their data sets and, potentially, be integrated into their data sharing capabilities (e.g., a COI can build a new capability using another COI service that is already in place).

[2] Available at the following website: http://dides.ncr.disa.mil/mdregHomePage/mdregHome.portal

C3.3.3. Forward Planning. COIs should plan for the long-term maintenance of COI metadata artifacts, including taxonomies and schemas, in consideration of other organizations that have built services that depend on these artifacts. For COIs that are not planned for long-term continuation, the COI should consult with the lead DoD Component organization or governing authority to develop a plan for long-term maintenance, to include CM.

C3.4. CAPABILITY PLANNING AND USER EVALUATION

C3.4.1. Activity Area Overview

C3.4.1.1. COIs play a key role in implementing net-centric data sharing across the Department of Defense. The mission-focused and typically joint nature of COIs enable the identification and development of net-centric information sharing capabilities that are of greatest value to DoD users. Through pilots and operational information sharing capabilities, members of COIs can demonstrate the mission value of using cross-Component data sources.

C3.4.1.2. The capability planning and user evaluation activity area focuses on defining an information sharing capability that the COI needs, working with DoD Components to implement the capability, and integrating it into ongoing operations. In some cases, COIs, through their members and associated programs, systems, and data sources, may develop pilot capabilities before engaging in full deployment of a capability. When planning for information sharing capabilities, COI members should define a set of requirements for the capability developers (associated with a Program of Record (PoR) or organization with data assets and budget). Associated PoRs inform DoD processes as appropriate when planning for information sharing capabilities. Capability developers are responsible for turning the requirements into a physical implementation of data assets and services in accordance with COI agreements.

C3.4.1.3. The overall goal of these activities is to assist a COI to evolve net-centric information sharing capabilities. Through these activities, COIs should actively identify information sharing needs and work to integrate new capabilities supporting known needs of the COI, as well as providing readily discoverable and understandable information to authorized but unanticipated users.

C3.4.2. Implementation Activities

C3.4.2.1. Identify the approach for delivering the capabilities. COI members must consider the normal certification and test processes when determining whether information sharing capabilities will be piloted or offered for operational use. The COI should base its approach on many factors, including technical and operational risk and the life-cycle stage of the data assets involved. For example, a COI may decide to develop a pilot capability that exposes data from existing systems in order to create a new asset before pursuing operational fielding of the capability. Leveraging exposed data from existing systems (instead of targeting programs in the new acquisition/development

cycle), may enable the COI to field a capability faster and provide more immediate benefits to users.

C3.4.2.2. Define measures of success. The COI's members should identify measures of success, including performance and resource-usage improvements. These measures should include metrics that can be used to assess the operational performance as well as provide insight into possible improvements in capability delivery (e.g., time to field, impacts on existing assets). When choosing to implement a pilot capability, it is important to assess whether the pilot effort will generate the intended capability to support the COI's mission, and whether the pilot capability technical solution can be integrated into the operational capability with a minimum of integration difficulty.

C3.4.2.3. Create a capability plan. COIs, in collaboration with the appropriate stakeholders, should develop a capability plan, including a schedule and identification of the data assets of programs, systems, and organizations to be tagged and exposed. Additionally, the plan should include resource requirements; any intermediate demonstrations, pilot efforts, and tests that must be performed; and operational integration tasks. The capability plan should be communicated with the governing authority, system and data asset owners, and other COI stakeholders. Implementation of the plan can then be carried out by participating programs and their respective capability developers. Communications should include measures of success to evaluate capability implementation and user satisfaction.

C3.4.3. Forward Planning

C3.4.3.1. Evaluate the capability. During capability execution, COIs should extend success criteria to evaluate the overall impact of the information sharing capability on the mission objectives and the overall value of the effort to the Department of Defense. The COI should evaluate capability planning and execution in two ways, which are described in subparagraphs C3.4.3.2. and C3.4.3.3., and then capture lessons learned, as described in subparagraph C3.4.3.4.

C3.4.3.2. Develop measures and metrics. In addition to metrics developed through the capability planning effort, COIs should develop metrics to assess the COI's progress relative to the DoD goals of net-centric information sharing and whether implementation resulted in a meaningful return on investment (ROI). In this instance, ROI indicates that the benefiting DoD Component or PoR has saved money by not having to build a new system to handle and re-create newly shared data. Other measures of ROI could include reduced cycle time and improved legal compliance. The COI should document the costs of implementation to provide a measure of the investment and should include a baseline assessment of relevant data assets to determine future capabilities.

C3.4.3.3. Check user satisfaction. As part of the ongoing feedback loop, COIs should make data regarding the information sharing capability implementation available and accessible to consumers of the community's data, and gather input from these users.

Gathering consumer, or user, input will enable the COI to gauge user satisfaction and determine whether the capability meets user needs and expectations.

C3.4.3.4. Capture lessons learned by the COI. Capturing and communicating lessons learned is a key part of the COI's governance responsibilities. Lessons learned provide current and future best practices, baseline financial data, and provide other valuable insight into the fielding of new information sharing capabilities. Although there is no one-size-fits-all approach, COIs should leverage all available resources to avoid repeating past mistakes and duplicating current efforts. COIs should also plan to meet regularly with the appropriate portfolio manager and other stakeholders to review implementation results.

C4. CHAPTER 4

DATA SHARING IMPLEMENTATION

C4.1. CHAPTER OVERVIEW

C4.1.1. Making data visible, accessible, understandable, and promoting trust are the cornerstones of net-centric information sharing. The creation of duplicative data and redundant capabilities often results from consumers' inability to locate, access, understand, or trust that existing data assets meet their needs. This chapter describes activities to guide COIs in implementing information sharing.

C4.1.2. The activities described in this chapter should not be interpreted as a rigid sequence. Some tailoring of the associated activities by individual COIs is expected and encouraged. Regardless of the steps taken, COIs should strive to fulfill their primary responsibilities, as shown in Table C2.T2.

C4.2. MAKING DATA VISIBLE

C4.2.1. Activity Area Overview

C4.2.1.1. Making data visible focuses on creating discovery metadata and deploying discovery capabilities that catalog data assets for users to find. The overall goal of data visibility is to enable DoD users to sift through the enormous volume and variety of DoD information holdings and quickly discover data assets that pertain to specific subjects of immediate interest. Discovery capabilities providing discovery metadata enable consumers to find out who is responsible for specific assets, where the assets are located, what kind of data is available, and how to go about accessing them.

C4.2.1.2. The discovery metadata may also include elements defined as COI extensions described in Reference (c). These elements are related to the subject matter of the data asset, and are necessary for specialist consumers in a particular subject matter to locate relevant data assets. The activities presented in the following paragraphs help implement policy goals of section 4.2. of Reference (a).

C4.2.2. Implementation Activities

C4.2.2.1. Identify data assets to share. Members of the COI should build a prioritized list of the data assets it will initially make visible to the Department of Defense. The list should include descriptive information on each of the identified data assets such as POC information, including email addresses and telephone numbers; name of proposed or existing data access service and any related information resources; and a high-level narrative description. The primary candidates for the initial visibility effort should be the COI's current operational data assets, followed by mature developmental capabilities that are on a rapid deployment track to fill known mission data gaps and information needs. Prioritization occurs at the COI's discretion, taking into consideration organizational preparedness, technical ease of service implementation, law, policy and

security classification restrictions, impact of broader access on the COI's operations, and the quantitative and qualitative improvements that might result from making a particular data asset visible.

C4.2.2.2. Define and register COI extensions for discovery metadata. One core purpose for COIs is to foster agreements on the meaning and physical representation of their data assets, as packaged and offered in deployed services. This includes the agreement on any metadata necessary to properly describe the community's data assets. Reference (c) provides the minimum discovery metadata requirements to support enterprise discovery of data assets and can be extended by COIs to provide additional context that aids in the search for relevant data assets.

C4.2.2.2.1. Enterprise Considerations. The COI is in the position to anticipate how users might want to find data assets, in part based on the data assets' context or content. Supplementing the rudimentary discovery metadata elements, such as "Creator" or "Classification" found in the DDMS core, the COI extensions detail elements of discovery metadata that aid in enterprise-wide discovery of data assets related to that COI.

C4.2.2.2.2. Technical Guidance. COI extensions to the DDMS may take the form of a data schema, and as such should be registered in the DoD Metadata Registry, as part of the COI's set of agreed upon metadata artifacts. Formatting and technical guidance for COI extensions can be found in Reference (c).

C4.2.2.3. Leverage work from other COIs. COIs should leverage the DoD Metadata Registry to access guidance on technical, organizational, and procedural approaches to data asset publication. Other available information includes specific DDMS extensions registered by other COIs, data schemas for carrying product payload, taxonomies, and other data engineering artifacts. These models can provide a starting point for the COI efforts to reach agreement on common elements that will be important for users to discover COI data assets. Additional information regarding COIs that have registered metadata in the DoD Metadata Registry may be available in the COI Directory.

C4.2.2.4. Associate discovery metadata with data assets. The association of discovery metadata with data assets is also referred to as "data tagging" within the context of data visibility. Data visibility is enhanced through the use and publication of discovery metadata that describe data assets. The implementation of "data tagging" mechanisms may vary by data asset and granularity of description. COI members should discuss possible methods of associating discovery metadata with capability developers or establish a COI working group to consider the issue and provide recommendations. In this way, the COI can determine the appropriate methods for the types of data assets the COI makes visible.

C4.2.2.4.1. Enterprise Considerations. Extensible Markup Language (XML)-based discovery metadata is the most flexible means of sharing discovery metadata throughout the Department of Defense.

C4.2.2.4.2. Technical Guidance. To illustrate the distinction between physical and logical tagging and association of metadata, consider the example of a data asset in the form of a single file, such as a DoD Directive. Physically tagging a file would mean placing discovery metadata elements directly into that file, alongside its content. In contrast, logically associating discovery metadata with the file would involve creating a separate file, possibly XML based, containing discovery metadata that describes the file. Software automation of this task is highly recommended; however, the precise mechanism will depend on the type of data asset and granularity of description. Reference (c) provides the minimum required structure and content for discovery-related tags. By adhering to this specification for tagging, the minimum necessary discovery metadata to participate in federated searches will be available.

C4.2.2.5. Create a discovery capability containing discovery metadata. Each COI should consult its governing authority to identify the information and resources associated with providing a discovery capability that the COI can use for its discovery metadata. The purpose of a discovery capability is to provide DDMS-formatted discovery metadata in response to federated searches. Capability developers will then leverage the COI's discovery metadata in the discovery capability, allowing authorized users to discover the COI's data assets.

C4.2.2.5.1. Enterprise Considerations. COIs should consult the enterprise specifications for data asset discovery. By complying with these enterprise discovery specifications, the COI helps ensure the interoperability of its discovery capability with the discovery capabilities of other groups and, ultimately, helps enable Enterprise-wide federation of discovery services. Federated discovery services give authorized DoD users the richest set of data assets from which to discover relevant data to meet their mission needs.

C4.2.2.5.2. Technical Guidance. COIs can access the Defense Information Systems Agency Net Centric Enterprise Services visibility guidance,[1] which provides more specific technical guidance for discovery capabilities. COIs should use available and mature federated search specifications to ensure that discovery capabilities interoperate with the Enterprise properly. Enterprise discovery specifications also include requirements for service discovery. Service discovery metadata typically takes the form of a Universal Description, Discovery, and Integration (UDDI) description of a web service. COIs can also consult with other COIs, or other existing resources, for implementations of discovery capabilities and gain insights into the use of similar technology across the Department of Defense.

C4.2.3. Forward Planning. COIs should establish, as part of its plan for long-term maintenance of COI metadata artifacts, a plan for maintaining the discovery metadata, the COI extensions to the DDMS, and the service discovery metadata. The goal is to make data visible as soon as possible and to develop those resources over time. The COI should agree on a schedule and process for how it will maintain the discovery metadata, to ensure that the data is always the most current.

[1] Available at the following website: http://diides.ncr.disa.mil/mdreg/user/Visibility.cfm

C4.3. MAKING DATA ACCESSIBLE

C4.3.1. Activity Area Overview

C4.3.1.1. Making data accessible focuses on offering data assets over the network through commonly supported access methods. This goal of Reference (b) deals with providing methods for obtaining data that both humans and machines can use, except where limited by law, policy, or security classifications. While making data visible involves creation and use of discovery metadata, making data accessible refers to providing access to the underlying information provided by the data asset so that authorized DoD users can make use of it. Taking into account the "post before processing" paradigm (Reference (b), the COI should make data assets available as soon as possible and should not delay making the data accessible in order to complete processing of data prior to posting it. This section describes activities that aid in implementing section 4.3 of Reference (a).

C4.3.1.2. Individually negotiated interfaces between systems are brittle and inflexible; they support only the information transfers anticipated during development, not the "pull-on-demand" transfers that are a key part of net-centric data sharing. While point-to-point interfaces will continue to exist, Reference (b) emphasizes the need to transition those interfaces and implement new interfaces to support many-to-many information exchanges and authorized but unanticipated users. Data producers should make data assets accessible using web-based approaches, minimizing the need for predefined, engineered point-to-point interfaces wherever operationally and technically possible.

C4.3.1.3. Examples of making data accessible

C4.3.1.3.1. Providing a website displaying imagery for an Area of Responsibility for humans to use. (This example describes a method through which humans can get information.)

C4.3.1.3.2. Providing a web service through which a computer application can obtain imagery data in support of situation awareness. (This example describes a method through which a computer can retrieve raw sensor image data.)

C4.3.1.3.3. Providing a web service that an application can use to determine the flight trajectory of a missile. (This example describes a method for computer access to a process or calculation.)

C4.3.2. Implementation Activities

C4.3.2.1. Understand data sharing constraints. The COI should identify any existing policies, laws, or data classifications that would restrict access to the data across the Enterprise. Traditional data access mechanisms will contain many implicit rules indicating how systems respond to requests, based on how the requests fall into a predefined process for handling the requests. Therefore, in addition to identifying explicit restrictions on data access, the COI should also consider the potential for (and attempt to discern) built-in role-based access control systems. COIs should maintain awareness of evolving DoD IA, information security, and information sharing policies and incorporate them as appropriate into COI activities and implementations.

C4.3.2.2. Discover enterprise resources. The COI should leverage work products of other COIs, operational data access mechanisms that are available, and available net-centric interface standards and specifications.

C4.3.2.2.1. Enterprise Considerations. The COI can promote access mechanism reuse, and minimize the work required to obtain desired capabilities by collaborating with other COIs. In addition, the COI can make its own data accessible on an enterprise scale by adhering to existing technical standards. Interfaces developed using standard interface specifications enable COI-developed access mechanisms to exchange information readily with enterprise services resulting in wider access to the community's data assets.

C4.3.2.2.2. Technical Guidance. The Key Interface Profiles[2] are the set of documentation produced as a result of interface analysis that designates an interface as key; analyzes it to understand its architectural, interoperability, test and configuration management characteristics; and documents those characteristics in conjunction with solution sets for issues identified during analysis.

C4.3.2.3. Identify data assets to make accessible. The COI should determine which assets within the associated organizations, PoRs, subportfolios, etc., are likely to be of most value to those inside and outside the COI taking into account the potential for authorized but unanticipated users. The data assets that the COI makes accessible will typically be a necessary component of the new information sharing capability identified by the COI.

C4.3.2.3.1. Enterprise Considerations. Part of the value of net-centric information sharing lies in its ability to afford authorized but unanticipated users with access to data, as needed. Taking this into account, COIs should assess information sharing options with the understanding that there might be other consumers in the Department of Defense, external to the COI, who could make valuable use of the COI's data.

[2] Available at the following website: http://kips.disa.mil/

C4.3.2.3.2. Define requirements for access mechanisms. The COI should define the priority of and functional requirements for data access mechanisms. Depending on the situation, the COI may base these requirements on an existing data access mechanism or establish them as part of an ongoing implementation plan. In setting requirements for data access mechanisms, the COI should take into account the type of assets; the security, license, and privacy considerations; and the static, dynamic, or streaming nature of data change. The data access mechanism specifications should conform to any agreements put forward by the stakeholders and the COI.

C4.3.2.3.3. Technical Guidance. The specific technology architecture of data access mechanisms will depend on a number of factors, including the nature of the underlying data asset, whether humans or machines will consume the asset, and the operational scenarios that surround the asset's use. Preferred architectures will use web-based technologies based on open standards, such as web services, portals, and web pages using Hypertext Markup Language (HTML) and common web display standards. The DoD Information Technology Standards Registry (DISR), according to DoD Directive 4630.5 (Reference (f)), provides the minimal set of rules governing the arrangement, interaction, and interdependence of system parts or elements whose purpose is to ensure that a conformant system satisfies a specified set of requirements. The standards and guidelines in the DISR are stable, technically mature, and available via DISRonline.[3]

C4.3.2.4. Post descriptions of access mechanisms. Capability developers in the COI should publish metadata for any data access mechanisms to available service registries, so that both known and authorized but unanticipated users may discover the service and understand how to interact with it.

C4.3.2.4.1. Enterprise Considerations. Publication of access mechanisms has two enterprise benefits: the first is enabling unanticipated users to find the service; the second is providing all background information necessary to reuse the service, deterring the development of redundant services.

C4.3.2.4.2. Technical Guidance. In the case of web services, enterprise specifications should be consulted for the minimum service discovery requirements to enable enterprise-wide discovery of COI data services. For instance, additional information in the form of a UDDI description may be required to enable federated discovery and greater understanding of data services.

C4.3.3. Forward Planning

C4.3.3.1. Review systems for operational impact and scalability. COIs should not degrade system performance for critical operational users to make data accessible. In addition, access mechanisms should be engineered for maximum scalability.

[3] Available at the following website: https://disronline.disa.mil/a/DISR/index.jsp

C4.3.3.2. Develop expandable systems. Although such mechanisms need not immediately support the entire set of DoD users, they must be expandable to meet growth in demand.

C4.4. MAKING DATA UNDERSTANDABLE

C4.4.1. Activity Area Overview. Making data understandable focuses on reaching agreement on the meaning of information provided by data assets and making that understanding available to consumers through the DoD Metadata Registry. Data that is visible and accessible is still not usable unless it is understandable. Reference (b) provides for the existence of expedient COIs that may have diverse data needs, based on operational requirements. It is therefore not always safe to assume that data consumers will be familiar with what a COI's data means, the way it is structured, or particularly how it fits into the COI's operational context. Most important, it is not necessarily the case that all consumers will be using data in the same way or for the same purpose. For example, "a tank" in the Army might refer to an armored vehicle, whereas "a tank" in the Navy might refer to a storage device for fluids. Although the data producer's perspective might be reasonable within the producer's context, the consumer might have a very different purpose in mind. This section describes activities that aid in implementation of sections 4.4, 4.6, and 4.7 of Reference (a).

C4.4.2. Implementation Activities

C4.4.2.1. Discover enterprise resources. As part of developing a shared understanding of the COI's data, the COI should discover existing enterprise resources in order to maximize reuse of existing metadata artifacts.

C4.4.2.1.1. Gather existing semantic metadata. The DoD Metadata Registry will contain vocabularies, taxonomies, ontologies, conceptual data schemas, and other forms of semantic metadata from other COIs upon which the COI might base development of its own semantic metadata. In addition, the COI should discover existing semantic metadata among its members. In this way, the COI can start the process with a foundation in related semantics.

C4.4.2.1.2. Gather existing structural metadata. The DoD Metadata Registry also contains logical and physical data schemas that could aid the COI in forming structural representations that would be understandable to end-users. Data asset structure (such as whether dates are represented as normal, or as Julian dates) is an important aspect of understanding. By using the DoD Metadata Registry and consulting COI members, the COI can start the process with a foundation in related structures.

C4.4.2.2. Develop a shared understanding of COI data made visible. COI members, pooling subject matter expertise, should collaborate on several semantic metadata artifacts that are crucial for providing context and meaning to any COI data that is made visible and accessible.

C4.4.2.2.1. Agree on a shared vocabulary. The COI should use its own extensions to the DDMS as a starting point for the shared vocabulary. As a set of terms and definitions, the shared vocabulary should include any term used in the COI extensions, along with definitions that put these and other terms into proper COI context.

C4.4.2.2.2. Agree on a conceptual data schema. The conceptual data schema indicates high-level data entities. Its coverage includes any entities in visible COI data assets, as well as the relationships between those data entities. The conceptual schema's coverage area may include multiple data assets, requiring that the COI come to an agreement on how members will collaborate, possibly through a COI data working group, to develop the conceptual schema.

C4.4.2.2.3. Agree on a COI taxonomy. A COI taxonomy is a categorization hierarchy indicating generalization and specialization relationships between terms; a submarine is a kind of sea-based asset, and an Abrams M1A1 is a kind of tank.

C4.4.2.2.4. Enterprise Considerations. Metadata artifacts such as the shared vocabulary, conceptual data schema, and taxonomy will be necessary for data consumers to understand a COI's data and to relate concepts within it. These artifacts will play a vital role in allowing mediation between COIs. The conceptual data schema indicates the general data subject area for consumers who are attempting to discover data assets relevant to their purpose.

C4.4.2.3. Associate format- and content-related metadata. Content-related metadata is specifically aimed at providing content details, such as topics, keywords, context, and other information. Format-related metadata refers to how the data asset is formatted or represented. It is important that data assets use formats that are understandable to data consumers. The COI should agree on how these metadata elements will be associated with data assets, using the DDMS as the specification for guidance on specific elements that will be associated with data assets.

C4.4.2.3.1. Enterprise Considerations. Content metadata provides a basis for search engines to locate data assets by keyword or topic, and improves the human understandability of the data. Format-related metadata enables consumers to determine whether or not they can consume a data asset. COIs should avoid the use of less well known publication formats that require special software. A good, understandable publication format will be one that is widely known and for which no additional software for conversion to a more widely known format is required.

C4.4.2.3.2. Technical Guidance. For content-related metadata, relevant DDMS elements are located in the Subject category. For format-related metadata, recommended formats are typically open and common throughout the enterprise, such as JPEG imagery, MP3 audio files, Apple Quick Time videos, and Microsoft Office document formats.

C4.4.2.4. Register the Metadata Artifacts. Registration of semantic and structural metadata within the DoD Metadata Registry enables all users both anticipated and unanticipated to discover their existence, access them, and establish an understanding of the meaning and context of COI data.

C4.4.2.4.1. Enterprise Considerations. Registration of metadata artifacts enables unanticipated users and those outside the COI to discover the meaning and context of COI data and facilitates their reuse across the Department of Defense.

C4.4.2.4.2. Technical Guidance. Registering these artifacts means posting them to the DoD Metadata Registry. The COI can accomplish this by accessing the DoD Metadata Registry and following the instructions for submission.

C4.4.3. Forward Planning

C4.4.3.1. Determine how the COI will maintain metadata artifacts. As the COI develops over time, the shared vocabulary, COI taxonomy, and other metadata artifacts that enable understandability should remain synchronized with the subject area they represent. To help it attain this objective, a COI could institute rules relating to how shared vocabulary updates occur. In addition, COI governance should be consulted for CM standards and related maintenance schedules.

C4.4.3.1.1. Enterprise Considerations. Unanticipated users will require and rely on up-to-date metadata artifacts to help them understand the context of discovered data assets and properly assess their relevance to their current mission.

C4.4.3.1.2. Improve the understandability of the data. The first iteration of metadata artifacts for understandability need not be ideal, since the goal is to make data assets available as soon as possible, rather than to have a perfect vocabulary on the first try. COIs should plan on improving their artifacts over time. Understandability is improved by providing more and better semantic metadata artifacts that capture and convey the knowledge consumers require to correctly use the data.

C4.4.3.2. Anticipate future mediation needs. Mediation is the process of reconciling one vocabulary with, or translating one vocabulary to, another. The need for such mediation is inevitable in an environment with many different systems and representation languages. By tracking which types of mediation occur or will occur most frequently, the COI can aggregate best practices surrounding the mediation of its data with other sources, as well as gain an understanding of what format and structural issues may exist. The COI should register metadata artifacts necessary for mediation in the DoD Metadata Registry, which will facilitate their discovery and usage.

C4.4.3.3. Ensure that data structure meets the consumers' needs, including those of unanticipated users. The physical structure of the data affects how the consumer will understand and utilize the data. Because it is not possible to know the unanticipated uses and needs of the data, COIs can engage in ongoing planning to change the structure of the data as it is exposed to the consumer via the access mechanism. Note that this sort of change represents a change to the access mechanism, not necessarily a change to the underlying data asset. Such changes can be meaningful only if they are made with consideration for user feedback.

C4.5. PROMOTING TRUST

C4.5.1. Activity Area Overview

C4.5.1.1. A consumer that can locate, access, and understand a particular data asset, will want to assess the authority of the data asset to determine whether the contents can be trusted. Promoting trust focuses on identifying sources clearly and associating rich pedigree and security metadata with data assets to support the consumer's trust decision.

C4.5.1.2. While COIs can promote trust through implementation of the activities described in this section, this Guide does not provide COIs the authority to share information in any way that is prohibited by law, policy, or security classification. This section describes activities that aid in implementation of section 4.5 of Reference (a).

C4.5.2. Implementation Activities

C4.5.2.1. Identify authoritative data sources. The COI should make every effort to identify data assets that are authoritative sources for data, as well as identifying in what contexts the data is authoritative. In situations where there is more than one authoritative source, depending on how the data is used, the COI should indicate the business process for which the authority is valid.

C4.5.2.1.1. Enterprise Considerations. The COI should consider the ownership and stewardship of data sources when determining authoritativeness. Active stewardship will help maintain the quality and relevance of authoritative data sources for those internal and external to the COI.

C4.5.2.1.2. Technical Guidance. Authoritative sources may vary by COI (e.g., one community may define an authoritative source for location data to be the United States Postal Service, whereas another community might define an authoritative source for location data to be an intelligence database). In addition, a community might define more than one authoritative source for a particular type of data (e.g., a budget and planning community might have an authoritative source for budget data for each Military Department).

C4.5.2.2. Associate trust discovery metadata with data assets. The COI should include trust discovery metadata to support data consumers' decisions on which community data assets are appropriate for their use. There are three categories of trust discovery metadata. These are discussed in the following subparagraphs.

C4.5.2.2.1. Asset pedigree metadata. The source and lineage of an asset are its pedigree. The purpose of the pedigree is to enable consumers to determine whether the asset is fit for their intended use and to enable them to track the flow of information, its transformations, and modifications, through assets. Notional metadata describing an asset's pedigree would include creation date, modification date, processing steps (including methods and tools), source and author (if known) status, and validation results against a published set of constraints.

C4.5.2.2.2. Security labels. Security labels provided in discovery metadata enable services to restrict access to data assets on the basis of a COI's identified parameters, including classification and dissemination controls. Preventing unauthorized access to data assets is important to promote trust in the data among authorized users.

C4.5.2.2.3. Associate rights protection metadata. Rights protection metadata refers to metadata that indicates any copyright, trademark, licensing, proprietary information, privacy act, or other usage restriction. As such, it may not be appropriate for all assets. Nevertheless, where this metadata does apply, it is important that it be provided. Consumers and data access services can only protect data against inappropriate use if they are informed of restrictions.

C4.5.2.2.4. Technical Guidance. The DDMS references the security elements found in the Intelligence Community Metadata Working Group document, specifying 18 attributes that can be used for information in classification and controls marking. The DDMS category named "Security" contains relevant elements addressing classification and dissemination. The "Source" category contains elements for asset pedigree metadata, and the "Rights" category contains applicable elements for rights protection metadata. The COI can obtain background on security tagging by checking the IC Metadata Standard for Information Security Markings (IC ISM) and accessing the Data Element Dictionary.[4]

C4.5.3. Forward Planning. Because a data asset can be trusted only if its contents are sufficiently accurate and of sufficiently reliable quality, assessing and improving data asset quality is important. 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 trustworthy, or they might need to know how accurate estimates and figures within the data asset are. Typically, such metadata results from a separate data quality analysis of an asset. The COI may develop an ongoing process for auditing the quality of data assets that are made visible and accessible. This process should be designed in concert with the COI leadership's ongoing quality assurance and CM efforts.

[4] Available at the following website: https://www.icmwg.org/ic_pub/index.asp