

Communities of Interest in the Net-Centric DoD Frequently Asked Questions (FAQ)



**May 19, 2004
Version 1.0**

Prepared by
The Department of Defense
Chief Information Officer
Information Management Directorate

Index of Questions

Introduction	3
Q1: What is a COI?	3
Q2: Why would a COI form?	5
Q3: How will the concepts of the Data Strategy be formalized within the Department and what will that do for the COI?	5
Q4: How are COIs funded?	6
Q5: What things should a COI do?	6
Q6: What things might a COI do to be effective?	7
Q7: How are COIs related to:?	7
Q8: How should COIs work within the Domain governance process?	8
Q9: What are the criteria for qualifying as a COI?	9

Introduction

The DoD Net-Centric Data Strategy outlines the vision for managing data in the Net-Centric environment known as the Global Information Grid (GIG). The Net-Centric goals that drive the Data Strategy focus on empowering users by ensuring all data are visible, accessible, and understandable across the GIG. To achieve the Net-Centric data goals, the Data Strategy acknowledges that there are formal and informal constructs within the Department for managing data. The formal construct uses DoD Issuances, such as directives to instruct DoD Components on their responsibilities with respect to achieving the data objectives. Informal collaborative constructs, such as working groups, task forces, and tiger teams contribute greatly to shared information within the Department and therefore will also be used to achieve data objectives. The Data Strategy uses Communities Of Interest (COIs) as the general term to describe the collaborative constructs.

The document is written in the “Question and Answer” format to address Frequently Asked Questions (FAQ) pertaining to COIs, and to convey lessons learned in the Department’s drive toward Net-Centricity. This “living” document addresses both current and future capabilities envisioned to support COI information sharing activities and will be updated as needed. It will be posted to the shared space via the GES Portal (<http://ges.dod.mil>) and the Assistant Secretary of Defense Network Information Integration (ASD (NII)) public home page (<http://www.dod.mil/nii/>)

NOTE: It is important to note that the scope of this FAQ is limited to COIs and their *relationship to data activities* in the Net-Centric DoD environment.

Q1: What is a COI?

COI is a term used to describe any 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. The COI concept is very broad, and covers an enormous number of potential groups of every kind and size. Any element of a DoD Component, e.g., domain, organization, task force, project team or group who must exchange information may be considered a “COI”. For example, every task-oriented workgroup (e.g. the bomb damage assessment cell at the Air Operations Center) can be a COI. Any collection of people with a declared interest (e.g. in biological warfare) can also be a COI.

COI membership may include various data owners and producers (e.g. developers, program managers, subject matter experts, users, etc.) that need to share the same semantic knowledge. Participants may represent organizations outside of DoD (NASA, Department of Homeland Security, etc.), or allied and coalition partners (NATO, Japan, etc.). A COI has the latitude to define an appropriate mechanism to manage COI membership. COI membership can be voluntary or mandatory depending on the roles of the participants. A participant’s involvement may change throughout the lifecycle of the COI. Initial membership may include the managerial level at the Joint Staff, Military Services, broad OSD representation, selected Defense Agency and Combatant Commands. However, as the effort progresses from the planning stage to a more technical focus, the membership may require greater technical and functional representation. For example, if you think your COI will impact acquisition, then acquisition organizations should be

encouraged to participate. COIs have the flexibility to engage a range of known participants at various intervals throughout COI lifecycle activities to ensure user requirements are adequately addressed. The chartering process may be a mechanism to solicit the appropriate membership at all levels, as needed.

COIs can exhibit a diverse range of characteristics depending on the community’s mission or objectives. The figure below illustrates some of the more prevalent COI characteristics and descriptive terms such as “Expedient”, “Institutional”, “Functional” and “Cross-Functional” used to characterize COIs.

COI Characteristics

Expedient	Tactically driven, Implied authority, Formal processes modified for need, Relatively many entities (e.g., New Imagery Analysis capability for Damage Assessment)	Tactically driven, Derived authority, Ad hoc processes, Many entities (e.g., Forward deployed JTF planning New Threat Response)
	Explicitly recognized, Longer term, More formalized processes based on span of control, Relatively few entities (e.g., PSAs such as Logistics)	Explicitly or implicitly recognized, Longer term but priority driven, Blended processes resulting from agreements (e.g., JS area such as Battlespace Awareness)
Institutional	Functional	Cross-Functional

Expedient COIs typically exploit existing resources (data assets) produced and exposed to the enterprise for discovery and reuse. These resources include vocabulary, developed applications, and other data assets. An example of an expedient COI may be a joint task force that uses data available to the network to generate new intelligence and planning scenarios. Institutional COIs tend to conduct activities such as develop vocabularies to provide a common understanding of terms used within the community, develop logical data models, register community specific extensions to discovery metadata schemas, and identify other data-related capabilities and services. An example of an institutional COI might be a health affairs community that is defining shared medical codes for Department wide use. Cross-Functional is the idea of Functional Areas, for instance, Health Affairs, Personnel & Readiness and Environmental working together to address data issues or topics that cross the boundaries of a single Functional Area.

Another way to characterize COIs is the persistence of the data or activities. Certain COIs may convene just a few collaboration sessions to complete their tasks, while longer term COIs may persist for years because there is a continuing need for their mission. It is up to the community members or the tasking authority to determine how long a COI should persist.

Q2: Why would a COI form?

A COI is formed whenever someone or a group decides there is value in establishing a community. For instance, someone with authority could direct the formation of a COI team to work a specific issue or individuals from different organizations could voluntarily form a COI team to address an issue that is common to the organizations. COI formations may occur in a "bottom-up" fashion, through the voluntary cooperation of the participants. They may also be formed through a "top-down" tasking.

An example of a "top-down" COI is Global Force Management (GFM). The challenge facing them was that DoD could not provide accurate, timely and authoritative GFM data to senior leadership regarding current locations, operational availability, and event data, among other data. As a result of this assessment by the J8 and others dealing with GFM issues, the GFM COI was established at the direction of the Director J8, Joint Staff. The USD (P&R) accepted to co-chair the effort and further the Defense Readiness Reporting effort.

Q3: How will the concepts of the Data Strategy be formalized within the Department and what will that do for the COI?

ASD (NII) will provide guidance and strategic support to DoD Components as part of a Department wide collaborative effort to institutionalize the Data Strategy concepts, such as facilitating data sharing through COIs and ensuring that a governance structure is in place so that COIs can form and operate effectively (see Q7, Q8). Guidance will be in the form of DoD issuances, which may include directives, procedures, handbooks, or manuals to formalize the implementation of net-centric policies. For example, the DoD Net-Centric Data Sharing Directive and supporting issuances are currently under development with an anticipated formal coordination of the Directive in June 2004. The issuance on COIs will provide generic guidance in regard to the establishment of COIs, to include the appropriate reference Department documentation and instructions, both for education and guidance. This COI FAQ documentation will be updated as needed to address COI related questions.

Formalizing the DoD Net-Centric Data Strategy content in DoD issuances will codify the COI concept thereby making it a recognizable entity within the Department. The issuance will recognize the COI as an entity(s) to participate in the Department's net-centric environment via the Domain governance process. Strategic support to the COIs will take form in a variety of activities and initiatives such as publishing discovery specifications to increase data asset visibility, developing a data asset catalog specification (future) to identify and locate data assets, developing an Enterprise COI Directory (see Q6) to provide visibility and collaboration with COIs.

An additional activity to promote the COI concepts may be to host a semi-annual COI conference, symposiums or colloquiums to discuss matters of mutual interest, and provide future direction regarding DoD CIO data strategies, policies and procedures, share lessons learned, etc.

Q4: How are COIs funded?

There is no central pot of "COI funds". DoD Components must continue to budget/plan and manage their resources to include data according to the guidance of the Planning, Programming, Budgeting, and Executing (PPBE) processes laid out by the Department".

If a COI is established through a Domain, the Domain portfolio management process will ensure resources are allocated to support the COI activities. COIs that form without being directed by a Domain should align themselves with an appropriate Domain(s) to leverage the capabilities provided by Domains.

Q5: What things should a COI do?

While COI members are working together to accomplish their shared objectives, there are additional data and information-related activities that they are encouraged to do in order to support the net-centric environment.

1. Make their data assets visible and accessible

Data owners/producers are responsible for making their data assets visible, accessible, and understandable. COIs can “expose” their data assets within the COI or across the Enterprise by tagging their data assets with discovery metadata, and posting those metadata to searchable catalogs. Posting metadata to a searchable catalog allows the authorized catalog user to browse the catalog, locate the data asset and learn enough information about the data asset to determine whether the associated data asset(s) fulfill the user’s needs. Data asset owners who are not part of a COI may work with one or more COIs to negotiate shared metadata development/catalog ownership or negotiate with an existing catalog owner to host their discovery metadata.

All discovery metadata shared with the Enterprise must be DDMS-compliant to ensure data assets are consistently described to aid the Enterprise-wide discovery capability. For information on the DDMS, please visit the [DoD Metadata Registry](#) and follow the [DDMS information link](#).

2. Define COI-specific vocabularies and taxonomies

Shared vocabularies and taxonomies promote the semantic and syntactic understanding of data assets.

Vocabularies include terms common within the COI and the associated definition of each term. Vocabularies help people understand what terms mean within that community. Vocabularies should also be developed to support machine-to-machine understanding of data elements. Taxonomies are categorization and classification schemes that the COI uses to group and relate its data assets. COIs are encouraged to develop and share vocabularies and taxonomies that best reflect the community’s understanding of their shared data. Both vocabularies and taxonomies should be registered in the DoD Metadata Registry to increase metadata visibility across the Enterprise and to promote possible reuse.

3. Register semantic and structural metadata to the DoD Metadata Registry

It is important that data structures, data definitions, data models, and other forms of semantic and structural metadata are registered in the DoD Metadata Registry for visibility and reuse. In doing

so, other communities and users throughout the DoD can find related constructs used to develop systems and to exchange information. By reusing existing metadata, systems and exchange formats tend to require less mediation or transformation. Additionally, by posting metadata to the DoD Metadata Registry, COIs can work together to converge on metadata specifications/standards that support many functions across the Department.

Q6: What things might a COI do to be effective?

In addition to the activities described in Question #5, there are additional activities that may be of value in supporting the COI's mission.

- Develop COI standard briefing to include at a minimum the COI problem set, requirements, architectures, membership, tasks ahead and roadmap to achieving the tasks. This briefing may serve as an educational tool for users to:
 - 1) Understand the CIO vision, problem, and timeline for implementation.
 - 2) Identify requirements for the COI to include data requirements.
 - 3) Understand what COI products will be produced.
- Develop a charter for their community. Objectives, persistent data service obligations, and large community memberships are some examples that may prompt a COI to consider developing their own charter to formally declare the scope of their mission, and define the rules and processes that govern their activities. The rules may entail managing changes to the community-defined metadata such as DDMS extensions, shared vocabulary, etc.
- Identify requirements for new capabilities, services or content and feed those requirements into the governance processes via the Domain owners (see Q7). Such community feedback will help refine future net-centric support for COIs.
- Inventory data assets that fall within the sphere of interest of the community so that they can readily be “tagged” and exposed. By producing this inventory, COI members (data owners/producers/consumers) can then begin to identify other related data assets that may be of interest to them.
- Extend the DDMS for COI specific discovery metadata. The extensible layer of the DDMS allows the COIs to extend the core layers of the DDMS with COI specific discovery metadata to support their mission-specific metadata requirements.
- Register their existence and membership in an Enterprise COI Directory. The COI Directory is a future capability that will provide descriptive information about the COI, such as its mission and participants. COIs may benefit from advertising their existence in the COI Directory by making their mission known to a broader part of the Enterprise, thereby benefiting from possible increased assistance. Additional information on the COI Directory will be provided as it becomes available.

Q7: How do COIs relate to other entities?

Domains—Domains are defined as subsets of mission areas and represent a common collection of related, or highly associated, information capabilities and services. The domain manages portfolios of information capabilities and services. Portfolio management of information capabilities and services within domains improve coordination, collaboration, integration, and

consistency of processes and interfaces for information sharing. This portfolio management construct is used to influence investments, requirements, and acquisitions related to IT and NSS systems. Domains ensure necessary capabilities are planned (e.g., metadata catalogs, metadata registries, etc.) and in place to form and operate COIs effectively. Since Domains cover the entire Department, every COI should fall within the scope of one or more Domains and thus be able to leverage the capabilities provided by that Domain if needed. COIs who have requirements for new capabilities, services and/or content may put forward their requirement to a Domain owner to be moved through the requirements, acquisition and resource allocation processes. The Domain and COI may develop an agreement or process to help maintain COI products (e.g., common data model, COI-specific vocabulary, etc).

Mission Areas—Mission Areas are supersets of Domains, i.e., a larger scope portfolio of IT and NSS investments. Mission Area is a defined area of responsibility whose functions and processes contribute to accomplishment of the mission. (DEPSECDEF Memo, Subject: IT Portfolio Management, March 22, 2004). The term is identified here for completeness but Mission Areas will have little direct influence on COIs.

DoD Components—DoD Components relate to COIs and their members in many ways (e.g., users, data producers, process owners, system operators, system owners). They fund, develop and operate most of the systems that produce data assets. They can sponsor a COI by providing the resources (e.g., personnel, etc.) needed to accomplish the required tasks and are responsible for implementing the tools needed for “tagging” and posting of data assets; in particular, they may be members of a COI or they may use a COI’s registered metadata (e.g., if COI develops a logical model for translating between vocabularies used by the COI, then a developer may utilize that model for translation to share information with another system). COIs will promote the use of metadata, use of web services to expose data and the registration of metadata among these project managers, developers and system owners. COIs typically will have an “influencing” role rather than a directing role in regards to these entities.

Namespace Managers— Namespace, as it relates to the DoD Metadata Registry, is defined as collections of data constructs that share a common context. This context may be technical such as “Imagery” or operational such as “Messaging.” In essence, a Namespace (or group of related Namespaces) is organized around a community that is able to agree on a common vocabulary. Each Namespace has a manager who has a stake in the syntax, semantics and other conventions concerning a specific collection of metadata.

Namespace Managers are responsible for acquiring and governing metadata information resources for designated Namespaces (note: a single Metadata Manager may have authority over multiple Namespaces). They may establish and chair working groups as required to coordinate the metadata management activities. The Metadata Manager represents their COI in metadata working groups and are also encouraged to participate in industry groups developing vocabularies and other components pertinent to their areas of interest.

Q8: How should COIs work within the Domain governance process?

Every COI should be affiliated with at least one Domain to ensure necessary capabilities are in place to facilitate semantic understanding. COIs may be tightly coupled to a Domain (e.g., they are established by a Domain) or loosely coupled as a result of the communities' interest falling

within the scope of a Domain. For example, an institutional COI may be formally tasked through the sponsoring Domain or subordinate component(s); hence, the COI will need to operate through the portfolio management construct of their sponsor(s). Such COIs may have authority from explicit chartering, or implied authority as a result of existing Organizational structures (see Q7 on COI relationship to Domains).

The intent of Domain governance process is to leverage existing processes for defining, resourcing, and acquiring capabilities against the context of portfolios of related capabilities rather than by platform or program. Domains are responsible for ensuring the necessary capabilities to form and operate COIs are planned and programmed for, and assigned to a Domain manager. Institutional COIs work through Domain managers from their affiliated Domains to obtain the authority and resource to accomplish their mission. Expedient COIs may operate through implied or derived authority (loosely coupled to a Domain); however, if the COIs have a long-term operational focus, then they may need to work through their organization's chain of command to find their sponsors.

Specific details on how COIs will operate under the Domain governance and portfolio management processes are still being finalized. When the details become available, they will be collected and integrated in the COI FAQ.

Q9: What are the criteria for qualifying as a COI?

There are no specific criteria for 'qualifying' as a COI. Any group of users who must exchange information may be a COI. Also, there is no "special process" for designating or establishing a COI. The Net-Centric Data Strategy encourages COIs to take the initiative in providing the organization and maintenance construct.