Department of Defense

Implementing the Net-Centric Data Strategy Progress and Compliance Report

August 2006

Prepared by
DoD CIO

INTRODUCTION

The Fall 2005 Quadrennial Defense Review (QDR) highlighted the Department of Defense (DoD) Net-Centric Data Strategy (May 2003) as one of the critical enablers of enterprise-wide information sharing, an essential element in the Department's ability to conduct network-centric operations. As a result, the QDR report (February 2006) emphasized that the Department will "strengthen its data strategy to improve information sharing," and the **Program Decision Memorandum (PDM) III tasked Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) to "report on data strategy implementation progress and compliance status to the Deputy Secretary of Defense in July 2006."**

This report is a broad area review of the Department's implementation of the DoD Net-Centric Data Strategy as mandated in DoD Directive (DoDD) 8320.2 (December 2004). The findings and recommendations are based on input from a cross-section of the Department's organizational entities that are collectively responsible for ensuring implementation of net-centric data sharing across the Department. The detailed approach and supporting data for this report are provided in Appendix A.

KEY FINDINGS

The following are the key findings of this report with recommended actions for the Department to accelerate implementation of the Net-Centric Data Strategy to increase information sharing.

Finding 1: The value of the Net-Centric Data Strategy remains largely unrealized by the warfighter, business, and intelligence operators. The Department does not have a systematic process for measuring implementation progress against the Net-Centric Data Strategy goals, collecting empirical evidence documenting the value of the Net-Centric Data Strategy to the operator, or assessing unsatisfied data needs.

To date, policy and guidance have focused on implementing the Net-Centric Data Strategy goals through Departmental processes to define, acquire, and implement capabilities. Less attention has been placed on measuring the effectiveness of data sharing in the operational environment.

Initiatives such as Horizontal Fusion have successfully demonstrated the Net-Centric Data Strategy implementation benefit to the warfighter through evaluation of a time-sensitive targeting (TST) mission thread in a fully netted environment. Horizontal Fusion demonstrated a faster, more accurate, and streamlined TST execution at a lower resource cost, which in turn reduced risk to the warfighter and improved the likelihood of mission success. In addition, studies such as those conducted by the Office of Force Transformation have collected empirical evidence of enhanced quality of information and shared situational awareness as a result of information sharing and collaboration. Although these efforts demonstrated operational value, the Department still lacks a continuous, near real-time and repeatable method to collect empirical evidence of the Department's operational data sharing status.

As operational data sharing challenges emerge, the Department does not have readily available technical and operational expertise that can be leveraged across the DoD Components.[1] No

[1] Military Departments, Combatant Commands, and DoD Agencies are collectively referred to in this document as "the DoD Components."

support is available to assist operators as they encounter data sharing issues in the execution of their missions. The ability to directly obtain operator input and feedback would offer significant insight into the Department's data sharing needs and enable the Department to focus its data sharing implementation.

Recommendations

- Within 90 days, the DoD Chief Information Officer (CIO) will scope an enterprise-wide data sharing implementation plan to be developed in coordination with the Department. The plan will consider non-DoD federal and coalition partners. The plan should emphasize data sharing in the operational environment and include metrics to measure the effectiveness of data sharing.
  - The Commander, Strategic Command (STRATCOM) and Director, DISA, will plan for and establish an information sharing operations center that addresses implementation of the Net-Centric Data Strategy for warfighting, business, and intelligence operators. This center will assist operators, and the DoD Components that implement data sharing capabilities, as data sharing issues are encountered in the execution of their missions. The center will provide technical and operational guidance for resolving data sharing problems. Within 120 days, the Commander, Strategic Command (STRATCOM) and Director, DISA, in coordination with the DoD CIO and appropriate DoD Components, will initiate planning for the center to include a concept of operations to describe functions, roles, and responsibilities to operate and monitor data sharing capabilities, including definition and collection of continuous, near real-time metrics on data sharing to support operators and other decision makers.

Finding 2: Communities of interest (COIs) are being established but require greater cross-DoD Component participation to address data sharing problems that cross organizational boundaries. In addition, COIs lack a structured mechanism for informing the Department's portfolio management processes relative to information sharing decisions.

DoD Components are establishing COIs to facilitate information sharing across functional areas with a focus on DoD Component priorities. The Military Departments independently govern their COIs through the Air Force's COI Coordination Panel, the Army's COI Harmonization and Integration Forum, and the Department of the Navy's (DON) Navy and United States Marine Corps' (USMC) Functional Area COIs. These types of forums enable the Military Departments to recognize, establish, and reconcile their COIs in relation to their organizational mission needs and priorities.

The DoD Components lack the mature policies, processes, and incentives necessary to initiate and engage in joint[2] COIs to address shared data problems. In select functional areas, such as Logistics and Command and Control (C2), COIs may garner participation from across the DoD Components and within coalition forces and federal and non-government entities. For example, the Maritime Domain Awareness (MDA) effort is a joint community focused on an information sharing problem that extends across and beyond the Department's boundaries, to include federal and commercial entities. The DoD Components are more likely to participate in joint COIs when there are assurances that COI-defined data sharing agreements will be implemented in information sharing capabilities outside their purview.

[2] COIs with participation from more than one DoD Component are considered joint.

The Department's Mission Area (MA) leads[3] are just beginning to establish the horizontal mechanisms to ensure that shared data problems are addressed in joint forums as early as possible, and that COI-defined data sharing agreements are implemented by appropriate programs within respective MA portfolios. The Warfighting Mission Area (WMA) is publishing guidance that begins to illustrate the fundamental relationship of COI-defined data sharing agreements and recommendations to management of the WMA portfolio. The Enterprise Information Environment MA (EIEMA), through the PDM III-directed Core Enterprise Services (CES) study, looked at an initial portfolio of information sharing capabilities across six major programs. The study concluded that the benefits and value of these information sharing capabilities to the enterprise cannot be realized until they are leveraged in a DoD-level information sharing infrastructure. The EIEMA will use recommendations from the CES study to prioritize the implementation and provisioning of these capabilities in a DoD-level information sharing infrastructure.

These efforts represent significant progress toward establishing the necessary processes to identify, prioritize, and address the Department's information sharing needs. Evolving the processes to achieve the flexibility and agility necessary to field information sharing capabilities quickly is still a considerable challenge.

Recommendations

In accordance with the DoD CIO memorandum, "Data Strategy Implementation Report to the Deputy Secretary of Defense," (31 March 2006), MA leads will—

- ❑ Within 30 days, identify one or more cross-DoD Component information sharing problem within the respective MA portfolio and designate COIs that will address the opportunities. Consider problems for which net-centric data sharing capabilities can be implemented within 12–18 months, provide support to current operations and/or a transformational program, or return high value to the enterprise.
- ❑ Within 30 days of identifying COIs, designate a DoD Component lead for each COI.
- ❑ Within 120 days, establish a process for MA governance for COIs, including a structured mechanism for informing the Department's portfolio management processes relative to information sharing decisions.
- ❑ Within 120 days, provide an MA-specific plan for integrating and collecting metrics within the portfolio review processes. Metrics should assess both data sharing implementation and effectiveness.

Finding 3: The DoD Components are updating their respective policies and guidance to reflect the Net-Centric Data Strategy goals; they are focusing primarily on implementing the goal of understandability and require additional technical guidance to mature the implementation of the visibility and accessibility goals.

The DoD Components are integrating Net-Centric Data Strategy implementation activities into their respective policies, guidance, and ongoing initiatives, such as transformation plans, systems migration strategies, service-oriented architecture (SOA) strategies, enterprise architectures, and portfolio management processes. Implementation maturity varies across organizations with the majority of the Department's activities focused on making data understandable.

[3] Mission Area leads are defined in DoD Directive 8115.

The DoD Components have directed resources to making data understandable with an emphasis on COIs. To support COI understandability efforts, the Army has established an Army Data Strategy Center of Excellence to provide data management expertise. While significant resources are being applied to COIs and data understandability, the efforts to make the data visible and accessible are considerably less mature across the Department.

The DoD Components are researching and developing capabilities to enable data visibility and accessibility. These efforts have focused primarily on meeting the needs of their respective DoD Component or specific program. For example, the Marine Corps Enterprise Information Technology Services (MCEITS) portal is designed to provide enhanced visibility and access to Marine Corps data to authorized Marine Corps users. In addition, the Air Force initiated a Joint Automated Metadata Tagging Pathfinder to identify a best-of-breed approach to automatically create discovery metadata by searching the content of structured and unstructured data assets. This approach will enable visibility of data assets by allowing users to locate, retrieve, and consume information that had previously been unavailable. The Air Force initiated Pathfinder has gained support and participation from the other Military Departments.

Although DISA has developed a specification for enterprise-wide content discovery that is based on the DoD Discovery Metadata Specification (DDMS), there is little awareness of this specification across the enterprise. Hence, capabilities developed at the DoD Component level may not be compatible with the enterprise. Enterprise-level technical guidance for the development of capabilities that enable data visibility and accessibility needs to be widely available to the DoD Components. The guidance needs to address the mechanism for creating discovery metadata, including automated tagging, and include examples for publishing data in common formats. This will ensure that DoD Component capabilities are compatible with the enterprise and can be made available for enterprise-wide use.

Recommendations

- Within 90 days, DISA (for NIPRNET/SIPRNET) and the Defense Intelligence Agency (DIA) (for DoD JWICS users) will jointly publish a draft federated search specification (compatible with DDMS[4]). The federated search specification will describe two approaches for DoD Components to publish their discovery metadata: 1) directly to the central discovery service and 2) federating their discovery service(s) to the central discovery service.
  - Within 180 days of publishing the federated search specification, DISA and DIA will provide a reference implementation(s) of the federated search specification and stand up a central discovery service on their respective networks that implements the federated search specification.
  - Within 90 days, DISA will provide detailed technical guidance and use cases to describe how to make various data assets[5] accessible. DISA will provide the guidance to the enterprise information sharing support center (see Finding 1) to maintain.

---

[4] DDMS is also published as the *Counter Terrorism Information Sharing Standard (CTISS) for Resource Metadata: Application Profile for Discovery under Executive Order 13388.*

[5] Data Asset: Any entity that is composed of data. For example, a database is a data asset that comprises data records. A data asset may be a system or application output file, database, document, or web page. A data asset also includes a service that may be provided to access data from an application. For example, a service that returns individual records from a database would be a data asset. Similarly, a website that returns data in response to specific queries (e.g., www.weather .com) would be a data asset. A human, system, or application may create a data asset. (DoDD 8320.2).

- Within 180 days of availability of technical specifications and guidance above, each DoD Component will identify priority data assets, consistent with MA priorities, and provide a strategy for making them visible, accessible, and understandable. Implementation strategies will be reviewed at appropriate DoD executive forums.

Finding 4: The Joint Capabilities Integration and Development System (JCIDS); Defense Acquisition System (DAS); and Program, Planning, Budgeting, and Execution (PPBE) are overwhelmingly "program-focused" and do not provide needed models for identifying, acquiring, and resourcing net-centric information sharing capabilities.

Directives and instructions, such as the Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 6212.01D, DoDD 4630.5, DoD Instruction (DoDI) 5000.2, and DoDI 4630.8, describe how programs report compliance against the Net-Ready Key Performance Parameter (NR-KPP) contained in the JCIDS Capability Development Document (CDD) and in Information Support Plans (ISP). These policies require programs to describe their relationship to the enterprise from a systems perspective; however, there are only minimal requirements for programs to describe "how" their information is made accessible to the enterprise. These policy documents, against which programs are directed to comply, contain few verifiable elements of the Net-Centric Data Strategy.

The JCIDS Initial Capabilities Document (ICD), described in CJCSI 3170, does not require capability developers to address the data produced and consumed, nor does it require a strategy to make the program's data visible, accessible, and understandable to users throughout the Department. The current processes are also insufficient in guiding the DoD Components to address data issues through COIs that are intended to inform capability development. Similarly, the current version of DoDI 5000.2 does not specifically require programs to articulate their plans for making their data visible, accessible, and understandable. Data issues that are not considered early in these processes often result in costly retrofitting of concepts, documentation, and implementation. Recent updates to the JCIDS and DAS processes promote an early and much closer relationship between the capabilities identification and system acquisition processes. There is still more that can be specified in these policies to compel the DoD Components and program managers to identify data challenges early enough in the respective processes to adequately impact capability definition, system development, and program implementation.

In addition, programs are directed to provide an extensive set of DoD Architecture Framework (DoDAF) products that illustrate their relationship to the enterprise, but these products are currently developed to support system-centric integration. These architecture products were not intended to readily support the demand of authorized but "unanticipated" users for data assets inherent to a net-centric operating environment. CJCSI 6212.01D relies heavily on DoDAF architecture products in its description of the NR-KPP and compliance with DoD net-centric goals. DoDAF architecture products must evolve to enable net-centric concepts for making data visible, accessible, and understandable to known mission partners operating in a legacy environment as well as authorized but "unanticipated" users operating in the net-centric environment.

The production and sustainment of DoD Components' capabilities offered as services require acquisition and budgeting models that enable them to sufficiently scale to meet the needs of both known mission partners and unanticipated users. The Department's major decision processes do not

incentivize the fielding of information sharing capabilities with the flexibility and agility required by a net-centric environment.

Recommendations

- In the next update of the CJCSI 3170, the Joint Staff (J-8) will include a requirement for identifying potential data challenges early in the JCIDS capabilities analysis process (i.e., Pre-MS A and B) to be included as part of the ICD.
- Within 180 days, the DoD CIO, working with the Joint Staff (J-6) and Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), will initiate a review and synchronization of CJCSI 6212, DoDD 4630.5, and DoDI 4630.8, to ensure NR-KPPs and ISPs include appropriate compliance measures that reflect implementation of the Net-Centric Data Strategy as codified in DoDD 8320.2 (includes refinement of required architecture products and policies).
- Within 90 days, USD(AT&L) and the DoD CIO will include a requirement in DoDI 5000.2 for programs to describe in the Technology Development Strategy (before MS A) their approach for ensuring that data will be made visible, accessible, and understandable. In addition, both DoDI 5000.2 and DoDI 4630 will be updated to include a specific reference to DoDD 8320.2.

CONCLUSION

Since the publication of DoDD 8320.2, the DoD Components have made incremental progress in implementing the Net-Centric Data Strategy. They are tailoring implementation to their organizations, establishing COIs, and initiating the development of technical infrastructures necessary to support information sharing. Although incremental progress is being made, the principal challenge faced across the Department is the translation of policy into implementation that results in real value to warfighter, business, and intelligence operators.

The Department must augment policy and guidance with operator-level solutions, realize the value of information sharing in the operational environment, and jointly measure information sharing activities and capabilities to improve mission effectiveness across the Department.

APPENDIX A:
NET-CENTRIC DATA STRATEGY IMPLEMENTATION PROGRESS AND COMPLIANCE REPORT DETAILS

APPROACH

On 20 December 2005, PDM-III tasked ASD(NII) as follows:

> "(U) ASD(NII). Report on data strategy implementation progress and compliance status to the Deputy Secretary of Defense in July 2006."

The ASD(NII)/DoD CIO issued a memorandum, "Data Strategy Implementation Report to the Deputy Secretary of Defense," (31 March 2006) to request input from Mission Area leads, Military Departments, and select Defense Agencies. As a broad area review of the Department's implementation progress, the memorandum requested participation from the Department of the Army, Department of the Air Force, Department of the Navy, Defense Logistics Agency (DLA), DISA, DIA, Business Mission Area (BMA), WMA, DoD Intelligence Mission Area (DIMA), and the EIEMA. Although COCOMS were not specifically identified, the Joint Forces Command (JFCOM) contributed input from the operator perspective. In addition, the DoD CIO staff conducted a review of the Department's JCIDS, DAS, and PPBE processes with representatives from the Joint Staff (J-8), USD(AT&L), and Director, PA&E, respectively.

To assess compliance with the responsibilities in DoDD 8320.2, input to this report was based on four assessment categories: Net-Centric Data Strategy Goals, COIs, Institutionalization, and Recommendations. The assessment categories and associated questions were developed by the DoD CIO's office and vetted with representatives of the Military Departments, DoD Agencies, and Mission Areas. The DoD CIO's office used the assessment questions to facilitate a series of interviews conducted with representatives from the organizations identified above. Interviews were conducted down to the program level to support the Department-wide scope for this report. The key findings represent an aggregate of a larger set of findings gathered through the course of the interviews. Beyond the key findings and recommendations given in the report, the DoD CIO recognizes that there are additional areas that need to be addressed to move the Department's implementation forward.

This appendix provides the details and additional anecdotal evidence collected from the interviews in support of the key findings summarized in the body of this report.

DETAILED FINDINGS

This section provides supporting details for each key finding and provides a more comprehensive view of the efforts to implement the Net-Centric Data Strategy across the Department.

Finding 1: The value of the Net-Centric Data Strategy remains largely unrealized by the warfighter, business and intelligence operators. The Department does not have a systematic process for measuring implementation progress against the Net-Centric Data Strategy goals, collecting empirical evidence documenting the value of the Net-Centric Data Strategy to the operator, or assessing unsatisfied data needs.

The ability to find the information needed, when it is needed, regardless of location, is key to net-centric operations and increases the warfighter's agility. Warfighters and other decision makers have yet to prioritize operator-level information sharing needs, and consequently, have yet to realize considerable benefits from data sharing. A few examples illustrate how the Department is attempting to move from policy to the operator.

- **WMA.** In accordance with the DoD CIO memo, "Data Strategy Implementation Report to the Deputy Secretary of Defense," (31 March 2006) WMA has developed an initial list of proposed WMA data sharing priorities based on WMA IT Domain Owner input. This list will be used to identify COIs and specify DoD Component leads that will begin resolution of highest priority operational data sharing problems.
- **EIEMA.** Horizontal Fusion demonstrated operator benefits of implementing the Net-Centric Data Strategy in several operational information sharing problem spaces. These include:
  - **Army's XVIII Airborne Corps**: In partnership with the Department of the Army and ASD/NII, the Army's XVIII Airborne Corps developed FusionNet to make battlefield information from all echelons available to warfighters at the tactical level.
  - **Joint Explosive Ordnance Disposal**: Improvised explosive device after-action reports from missions underway in Iraq, Afghanistan, and elsewhere can be shared and accessed.
- **DIMA.** DIMA identified "operationally relevant" missions as the key requirement for implementing data sharing. Although DIMA has not formalized its plans, its information sharing priorities include joint task forces such as international security assistance forces-Afghanistan, North American Treaty Organization information sharing, and other Coalition information sharing efforts.
- **Missile Defense Agency (MDA).** MDA will issue an MDA Master Data Management Directive. The proposed directive requires registration of all data assets accessible within the agency. The data can be collected and searched as appropriate based on the role of the individual accessing the MDA Metadata Registry via the MDA portal. Internal sharing is the priority, but data sharing beyond the bounds of MDA is a long-term consideration.
  - Discovery is particularly challenging. Given the magnitude of the effort to record all agency data assets, an automated tool is being designed to pull key metadata from sources automatically entered into the metadata registry. The Network Operations Monitoring and Asset Discovery aids in the collection of information on all agency network connected assets to identify potential creation and use of data assets.
  - Two proofs-of-concept are being established using automated tools, organization and storage, and presentation tools. They are: eWorkforce data gathering analysis and presentation, which integrates MDA workforce data from a wide variety of agency personnel systems; and eBusiness initiatives involving data discovery, authoritative data sourcing, data integration, data sharing, and work process simplification.

Although several activities in the Department focus on evaluating progress and compliance with data sharing initiatives, these efforts do not enable the Department to measure the effectiveness of data sharing from the perspective of the warfighter, business, and intelligence operators. Some efforts, primarily internal to organizations, are attempting to facilitate the collection of metrics; however, there is no enterprise-wide, repeatable method to collect empirical evidence of the Department's operational data sharing status.

- **WMA.** Through CJCSI 6212.01D, "Interoperability and Supportability Certifications," WMA will enable COIs to influence programs of record (POR) to implement data sharing capabilities by requiring them to report the Net-Centric Data Strategy and COI activities as part of the Interoperability and Supportability Certifications.
- **Army.** The Army developed a three-level plan to collect metrics. Initial Measures of Success/Progress of COIs include criteria at each step. The plan is intended to measure the success and progress of COIs at each level, where level one ascertains whether the established process is being followed; level two pertains to the quality of products, harmonization, and leveraging of products; and level three deals with implementation and support of COI products and agreements.

Finding 2: Communities of interest (COIs) are being established but require greater cross-DoD Component participation to address data sharing problems that cross organizational boundaries. In addition, COIs lack a structured mechanism for informing the Department's portfolio management processes relative to information sharing decisions.

The DoD Components are participating in and establishing COIs to solve data sharing problems, but they are largely focused on formation, management, and oversight within their organizational boundaries. The DoD Components lack the mature policies, processes, and joint incentives necessary to initiate and engage in COIs that span organizational boundaries.

- **Navy.** The 5000.36a SECNAVINST identifies 21 functional areas in the Navy. Each functional area operates as a COI and is working to establish the common Navy vocabulary for the respective functional area.
- **USMC.** The Marine Corps actively participates in several joint COIs, including Global Force Management (GFM) and Blue Force Tracking (BFT), and is assuming a leadership role with others. In addition to leveraging the Navy 5000.36 SECNAVINST, the USMC is institutionalizing data management by standing up a Data Strategy Working Group and a Data Strategy Center of Excellence that will address and implement the tenets of the DoD Net-Centric Data Strategy.
- **Air Force.** The Air Force champions the C2 Space Situational Awareness (SSA) COI that is working with six PORs to implement 40 data elements in the C2 SSA vocabulary and provide direct machine-to-machine communications.
- **Army.** The Army supports 18 COIs and/or data-related forums, including Strike COI, BFT, and the Joint NetOps COI. The Army chairs the data working groups for the BFT and NetOps COIs. The Army's approach to COIs focuses on developing multiservice collaborative groups to ensure that COI products support all DoD Components to the greatest extent possible.
- **DIA.** DIA is establishing COIs that include a high percentage of functional staff to ensure that COI membership will produce viable products for the COIs that they lead and participate in, including Intelligence Surveillance and Reconnaissance (ISR) COI, Battlespace Awareness Board, Intel-Ops Bridge, and Counter Intelligence/Law Enforcement Bridge.
- **DLA.** DLA recognized community-based information sharing groups for Focused Logistics and Supply Management. The DLA - Defense Logistics Management Standards Office (DLMSO) has registered the Supply Management COI with participation from the supply management community.

- **JFCOM.** JFCOM is involved in many COIs, some of which span functional areas; participation includes the ISR COI, the Joint Geospatial Intelligence Activity (a COI-like effort concerning geospatial intelligence), the Meteorology and Oceanography COI, the Force Projection COI, TST COI, BFT COI, Joint Air Missile Defense (JAMD) COI, and Joint Task Force (JTF) C2 COI, among others. JFCOM is participating in piloting information sharing capabilities, such as the Cross-Domain Collaborative Information Environment, which addresses cross-domain data sharing needs.
- **BMA.** The BMA's Business Enterprise Priorities (BEP) function as COIs and promote joint functional areas to achieve specific objectives, including data sharing initiatives. The BEPs include financial visibility, acquisition visibility, materiel visibility, personnel visibility, real property accountability, and common supplier engagement. These collaborative functional teams illustrate how the Department is addressing cross-organizational and joint COIs.
- **WMA.** Through the Joint Staff's experience in co-chairing the GFM COI they have identified the following issues related to COIs and implementing the Net-Centric Data Strategy: 1) common semantics need to be developed for the enterprise, 2) resources are not dedicated, 3) development of policy level guidance needs continued emphasis, 4) the Net-Centric Data Strategy does not adequately address nor solve the unique identification issues.

Although the MA leads are in the planning stages of establishing the mechanisms to address data sharing in joint forums, the DoD Components have established forums to formalize, manage, and govern their COIs. The following examples illustrate several forums that enable COI governance within individual DoD Components.

- **Air Force.** The AF's COI Coordination Panel was established to ensure that Air Force-led COIs and COIs the Air Force participates in provide value and are not duplicative efforts.
- **Navy.** The DON Data Management Governance Structure aligns the Navy's Data Management, Extensible Markup Language (XML), SOA, and COI activities and facilitates operations of COIs. In addition, the Navy has established the DON COI Collaboration Workspace (https://gesportal.dod. Mil/sites/DonCoiCollab) as the central site for coordinating initiatives and activities of various Joint, DON, Navy, and USMC COIs.
- **USMC.** The Marine Corps' Data Strategy Working Group and Data Center of Excellence are being formed as the governance and oversight bodies for COIs that are led by the Marine Corps or that interact with Marine Corps Commands, systems, data, or processes.
- **Army.** The Army established the Army Enterprise COI Forum as the mechanism for discussions concerning how the Army approaches COI formation, participation, and management. This forum acts as a liaison to other Services and the JFCOM COI Governance board(s), and to develop an infrastructure and repeatable processes, even across Services. The Army is evolving the COI Forum into the Army COI Harmonization and Integration Forum to manage and monitor the formation and execution of COIs that the Army is either leading or supporting. The Army is linking the Harmonization and Integration Forum to the Army Portfolio Management Governance Council for Army general officer oversight.
  - The Army has established the Army Data Strategy Center of Excellence to support COIs in the lifecycle of their activities. This center will facilitate the uniformed, efficient, and effective execution of COIs, their project management aspects and governance.

Although the Mission Areas are developing portfolio management processes and guidance, they are in the early stages of facilitating cross-DoD Component COIs. The following represents some of the emerging efforts from the Mission Areas to address cross-Component COIs.

- **WMA.** The WMA is working toward publishing CJCSI 8410, "Warfighting Mission Area (WMA) Portfolio Management (PfM) and Communities of Interest (COI)," which defines Domain Owner responsibilities for COI governance and portfolio management.
- **BMA.** The BMA is working to identify net-centric data sharing opportunities (including supporting metrics, data collection, and analysis) as part of the Defense Business Systems Acquisition Executive (DBSAE) initiatives. The DBSAE is collaborating with other Department resources to analyze the affinities of several DBSAE programs. The BMA will pilot information sharing capabilities based on this analysis and is planning for a service-oriented and data sharing environment for all DBSAE programs.
- **EIEMA.** The EIEMA established an Investment Review Board (IRB) to manage the Department's portfolio of infrastructure capabilities and investments. A key aspect of the portfolio processes will be the inclusion of COIs in the portfolio evaluation and selection process to ensure EIEMA capabilities are transforming toward a net-centric information sharing capability and incorporate key elements of the Net-Centric Data Strategy.
  - The PDM III also initiated a study of the Department's CES. The CES study included the following six major DoD programs: Net-Centric Enterprise Services (NCES); Future Combat System's System of Systems Common Operating Environment; Distributed Common Ground System – Air Force; Global Combat Support System – Air Force (GCSS-AF); MCEITS; and the National Security Agency CASPORT.
    - The CES study identified the following examples of information sharing capabilities that are limited to program-level information sharing infrastructures: content discovery services, service registry, access control and certificate validation, chat and presence awareness, and directory services.
    - The EIEMA IRB will leverage the CES study's recommendations on information sharing capabilities being developed to ensure they are appropriately leveraged into a robust DoD-level information sharing infrastructure. The CES study will make recommendations on the following: expediting the fielding of security services, fielding and populating an enterprise service registry, establishing enterprise directory services, and defining the capabilities of a service management CES.

Finding 3: The DoD Components are updating their respective policies and guidance to reflect the Net-Centric Data Strategy goals; they are primarily focused on implementing the goal of understandability and require additional technical guidance to mature the implementation of the visibility and accessibility goals.

As DoD Components adopt and tailor DoDD 8320.2 to their organizations, the following represent respective policies and guidance being updated.

- **Air Force.** The "Air Force Information and Data Management Strategy Policy," (03 March 2004) describes the Air Force vision for managing and leveraging information. It focuses on providing "Air Force personnel with on-demand access to authoritative, relevant and sufficient information to perform their duties efficiently and effectively."

  - The Secretary of the Air Force's Data Transparency Initiative is establishing the Transparency Integrated Project Team (IPT) so that Air Force data will be visible to all Air Force personnel, data is formatted and presented to the user in a manner that makes it understandable and allow sufficient transparency into processes that generate data for users to trust the information as displayed. The Transparency IPT provides guidance to the AF's COI Coordination Panel.
- **Army.** AR 25-1, "Army Knowledge Management and Information Technology Management," provides the policy foundation on which the Army will implement the Net-Centric Data Strategy. Implementation guidance is found in Department of the Army Pamphlet 25-1-1, Chapter 5, "Army Net-Centric Data Management;" the "Army Guidance for implementing the Net-Centric Data Strategy;" and the "Army COI Guidance" documents.
- **DON/USMC.** DON policy in SECNAVINST 5000.36A, "DON IT Applications and Data Management," addresses DoD Component-level Information Management through functional areas. The Navy is updating guidance on the use of XML by issuing the new DON XML Naming and Design Rules that guides the standardization of XML development and implementation within the DON.
- **Business Transformation Agency (BTA) (for the BMA).** The BTA has developed the Business Enterprise Architecture "Business Mission Area (BMA) Net-Centric Strategy," which addresses the Net-Centric Data Strategy's goals within the Business Community.
- **DLA.** The DLA Directive 5025.30, One Book Chapter Data/Information management is guidance for DLA to support Net-Centricity.

The majority of the Department's Net-Centric Data Strategy implementation activities are focused at the DoD Component level, specifically around semantics, vocabularies, and ontologies. The following illustrates how the DoD Components are focused on making data understandable.

- **Air Force.** The Space Command effort is implementing the C2 SSA vocabulary, developed by the C2 SSA COI, which will provide direct machine-to-machine communications within six PORs. The effort was established by the Air Force Transparency IPT.
- **Army.** The Army is creating a template for a COI Vocabulary Guide, developing the C4ISR Data Ontology, developing the initial XML schema for the BFT COI, and developing a change management plan that supports implementation of the Joint Command, Control and Consultation Information Exchange Data Model (JC3IEDM).
- **USMC.** The Marine Corps is developing a Marine Corps-specific ontology to be used internally and externally, across the DoD Components, to ensure semantic correctness within the MCEITS architecture.
- **BTA.** The BTA published the Standard Financial Information Structure Vocabulary in the DoD Metadata Registry. This vocabulary supports comprehensive corporate financial management and federal financial reporting that is consistent with the Chief Financial Officer Act and is being implemented at the DoD Component level.
- **DLA.** The DLMSO developed the Corporate Logistics Data Architecture that represents the set of logistics data elements under the stewardship of the DoD Logistics Functional Data Administrator. The data elements are structured, named, and defined in accordance with the ISO 11179 standard. The DLA Integrated Data Environment (IDE) uses the DDMS.

Although the findings provide many examples of implementing the goal of understandability, fewer examples were available with respect to implementing data visibility and accessibility. The following examples provide insight with respect to DoD Component pilot or implementation efforts for data visibility and accessibility.

- **Air Force.** The Air Force initiated a Joint Automated Metadata Tagging Pathfinder with Army, Navy, and Marine Corps participation. The pathfinder concept is to demonstrate commercial off-the-shelf technologies that automatically create discovery metadata values by searching the actual content of structured and unstructured information and knowledge-based assets with metadata values. The pathfinder is being conducted in two spirals. The vocabularies being used are from Financial Management (FM), Logistics, and JC3IEDM. C2 SSA and JAMD are being considered for inclusion. The data to be tagged will be in various media forms, including documents, briefings, and spreadsheets. The focus of the pathfinder is to tag information and knowledge-based assets with metadata that can be stored in a metadata repository and searched by users to locate, retrieve, and consume.
- **Army.** The Army Distributed Common Ground System (DCGS-A) program is working to make data assets visible and accessible. The DCGS-A is constructing a set of leveraged ISR web services-based interface specifications. These specifications conform to a standards-based approach and are built using industry open standards, such as XML.
  - The TRADOC, ARCIC, AIMD developed and implemented the Capabilities Assessment, Development, and Integration Environment (CADIE) which provides a collaborative, common environment for architecture related efforts in support of the JCIDS process throughout the TRADOC community and with the Army/Joint/DoD partners. The CADIE project has uncovered and helped resolve multiple issues with regards to network security, user authentication regulations and policy that effect information discovery, sharing, and collaboration across the DoD and Army architecture community.
- **DISA.** DISA developed a set of specifications and services for content discovery as part of the NCES Early Capabilities Baseline. This capability provides a standard approach for exposing DDMS compliant metadata to the Global Information Grid (GIG), and consists of two functional components: Federated Search and Enterprise Catalog.
  - The DoD CIO memorandum "Supporting Data Asset Visibility – Implementing the DoD Net-Centric Data Strategy (24 October 2003)," and subsequent action memorandum (27 July 2004), tasked DISA to provide the specifications to describe Enterprise Discovery functions and their interfaces to enable federation with DoD Component discovery capabilities. The recommendations in this report refer to this action, further emphasize the requirement for future versions of the specification, and for making it widely available to the Department.
  - The Net-Centric Command Capability (NECC) Net-Centric Capability Pilot activities in advance of Milestone A were discoverable using DDMS, and the subsequent NECC Pilot activities for Timebox 1 are planned to make all data assets within the technical architecture discoverable and DDMS compliant, with more emphasis on unanticipated user discovery. Nearly all of the programs within PEO-C2C programs have registered their XML in the DoD Metadata registry for some time now.
- **DNI.** The IC DMC (Data Management Committee) (formerly the Intelligence Community Metadata Working Group [IC MWG]) chartered a panel of representatives from the FBI, the Department of State, the National Intelligence Agencies, the Terrorist Threat Integration

Center, the DoD, and the DHS to establish a terrorist watchlist person data exchange standard. This joint community established a watchlist exchange data structure and schema which is currently being piloted by the NIEM (National Information Exchange Model) project. The NIEM project goal is to provide an "enterprise-wide framework to facilitate information sharing across all levels of government in support of justice, public safety, intelligence, and homeland security."

To better implement the Net-Centric Data Strategy, the DoD Components and Mission Areas require the technical infrastructure capabilities to enable visibility, accessibility, and understandability of data. Lacking a robust information sharing infrastructure, the DoD Components are planning for and developing their own information sharing capabilities.

- **USMC.** The MCEITS portal is designed to align IT resources to create a shared IT services and information environment and establish a reliable, secure, efficient, responsive IT infrastructure that provides enhanced information access and information management.
  - The Marine Corps' data architecture establishes governance procedures and policy guidance for Marine Corps Commands on data sharing in the USMC and across DoD.
- **Air Force.** The Air Force created an initial implementation of a Common Operating Picture capability to provide a user-friendly dashboard view of data services, which will aid in enabling information sharing.
  - The GCSS-AF program is currently developing a metadata catalog to facilitate DoD Component level search.
- **Army.** The Army Knowledge Online portal is the Army's enterprise-class portal and central point for secure access to information, data assets, and tools for Army personnel. This portal enables information sharing to a network-based force of more than 1.8 million users.
- **DISA.** The Defense Online portal is the service gateway to access information services on the GIG. The Defense Online portal includes links to the NCES Pilot Services that support information sharing, including security/information assurance, service discovery, enterprise service management, machine-to-machine messaging, people and device discovery, mediation, and metadata registry services.
- **DLA.** DLA is implementing information sharing capabilities through the Global Transportation Network, which partners with US Transportation Command to provide and enhance supply and transportation information. Additionally, DLA's IDE provides the infrastructure as a single point of access for DLA-managed data and data inbound to DLA, including commercial suppliers and across DoD.
- **BMA.** BMA is planning the technical infrastructure necessary for Net-Centric Data Strategy implementation by developing a BMA Federation Strategy, which will establish the vision of how the operating environment of BMA will enable data interoperability.
  - **BTA (on behalf of the BMA).** BTA is executing the Business Enterprise Information Service (BEIS) program to build upon existing infrastructure to provide timely, accurate, and reliable business information from across the DoD to support auditable financial statements as well as provide detailed information visibility for management in support of the warfighter.
    - The BEIS SFIS Library Service will communicate and distribute the SFIS vocabulary to the enterprise. The BEIS Master Appropriation Service will deploy web services to expose appropriation data from Department of the Treasury to the DoD enterprise.

Although an enterprise-level technical infrastructure is essential to support the implementation of the Net-Centric Data Strategy, technical guidance and support must also be available to facilitate implementation.

- **DoD CIO.** The DoD CIO has published DoD 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing" (12 April 2006) to provide functional implementation guidance.
  - DoDAF guidance and architecture products are being updated to address net-centric concepts and SOAs.

Finding 4: The Joint Capabilities Integration and Development System (JCIDS); Defense Acquisition System (DAS); and Program, Planning, Budgeting, and Execution (PPBE) are overwhelmingly "program-focused" and do not provide needed models for identifying, acquiring, and resourcing net-centric information sharing capabilities.

Changes made to the JCIDS and DAS processes mandate an early and much closer relationship between the two processes to enable better definition and execution of acquisition and capabilities identification process.

- **JCIDS.** The JCIDS contains some reference to net-centric goals; however, the guidance is not robust enough to compel capability developers to identify information or information service challenges early enough in the capability development process to properly shape capability definition, help program acquisition, and ultimately, assist in program implementation. The policies emphasize the necessity of integrated and interoperable joint warfighting capabilities and place emphasis on IT, including data standards, data sharing, and compliance with the DoD Net-Centric Data Strategy, yet these concepts rarely are presented in the required documentation.
  - JCIDS describes an analytic process for developing capabilities-based assessments (CBA). The capability developer uses CBAs to set the operational context and identify current capabilities, gaps, and redundancies, as well as potential materiel and non-materiel approaches to addressing the gaps. CBA results provide the basis for ICDs, CDDs, and Capability Production Documents (CPD). These documents provide the acquisition program manager the "capability blueprint" needed to develop a material solution. CBAs are conducted prior to MS A and usually produce an ICD by MS A. The CDD is required at MS B; and the CPD is required at MS C.
  - The JCIDS process provides minimal guidance that directs capability developers to identify information needs and a strategy for addressing them.
  - JCIDS does not require capability developers to identify required or produced information and information services and the associated COIs early in the capabilities development process. Hence, program managers remain uninformed during early acquisition activities, such as the Technology Development phase, and are unable to offer a greater advantage in achieving program goals.
  - The ICD development process does not facilitate early discussion of information needs, COIs, and a strategy to address them. JS-J8 JCIDS process owners emphasize that at the pre-ICD stage, many alternative solutions exist, so discussions of information needs and COIs will be general.
- **JCIDS/DAS**. Secondary documents supporting the JCIDS and acquisition processes, including CJCSI 6212, DoDD 4630.5, and DoDI 4630.8, describe how programs report

compliance against specific performance parameters described in the NR-KPP, Net-Centric Operations Warfare Reference Model (NCOW RM), and the ISPs. The CJCSI 6212.01D describes interoperability compliance for video, voice, and data, and necessarily describes point-to-point information exchanges.

- The DoDAF v1.0 supports CJCSI 6212.01D by identifying the architectural views required for compliance. The current version of DoDAF does not account for net-centric concepts and is based on end-to-end information exchanges. This results in enforcement of the Net-Centric Data Strategy within the NR-KPP as focused on legacy architecture views and architecture data. The DoD CIO is leading a Department-wide effort to update DoDAF, including changing content to align with Net-Centric concepts. The CJCSI 6212.01D should be updated to reflect net-centric goals as soon as practicable, particularly where it discusses net-centricity systems-to-systems and point-to-point information exchanges.
- Programs are directed to provide an extensive set of DoDAF architecture products to illustrate various aspects of a program's relationship to the enterprise (i.e., its operational and technical composition and function).
  - Program managers (PM) indicated that many of these products are overly complicated and not useful to developers, that architecture products should be developed that reflect the services used and the consumers of information produced, and that architecture products should be developed that require identification of data they are going to expose.
- The MS review process includes few verifiable elements of the Net-Centric Data Strategy (i.e., ability to expose the associated service/data to the GIG and the ability to access needed services/data on the GIG) against which programs are directed to comply.

- **DAS/PPBE.** The DAS and PPBE processes do not support the production and sustainment of data and data services, which require both proper financial funding models and budgeting for resources to execute with optimal efficiency. There is no Department plan that outlines how these elements will be provided to ensure that DoD Components can address the unanticipated user's needs.
  - The PPBE process owner, through the Defense Warfighting Capital Fund, is looking at ways to fund sustainment of services offered by a DoD Component that are available for broad, DoD-wide enterprise use, including the unanticipated users,
  - The office of the Director, PA&E, believes how the Department will fund capabilities as services, which are scalable to unanticipated users, should be studied and developed across the DoD enterprise.
  - Early identification of net-centric data plans in the TDS before MS A is not specifically required in current versions of the DoDI 5000.2 or in the DoDI 4630 series. The TDS describes the acquisition approach, rationale, and methodology for dividing the program into technology spirals or increments. It also discusses cost, schedule, and performance goals and exit criteria for the first technology spiral development program.
  - The DAS does not identify a requirement for early discussion of information sharing challenges. This omission poses an increased risk that appropriate technologies for implementing policies in DoDD 8320.2 will not be fully explored. Recommended changes to these documents to include early description of the programs approach to implementing the DoD Net-Centric Data Strategy in the TDS before MS A have been

agreed upon by USD(AT&L) and ASD(NII)/DoD CIO. The following changes to the DoDI 5000.2 and DoDI 4630 series are recommended:

1) DoDI 4630 series, insert in Table E3.T2

Add, and DoD Directive 8320.2 ….. and (br)	Program Initiation for Ships (first draft) Milestone B (first draft) Critical Design Review (CDR) (second draft) Milestone C (final)

2) DoDI 5000.2, insert in Statutory Information Requirements Table E3.T1

Add DoDD 8320.2	

3) DoDI 5000.2, insert a new paragraph at 3.4.4.5 as follows:

3.5.4.5. A description of the program's approach for ensuring data will be made visible, accessible, and understandable to any potential DoD user as early as possible. Updates to this information will be included in the ISP at subsequent Milestones for all programs.