Office of the Army Chief Information Officer/G-6

Army Data Strategy

February 2016

Information Architecture Division
Army Architecture Integration Center
HQDA CIO/G-6

Version 1.0

CIO/G-6
ENABLING SUCCESS For Today and Tomorrow

U.S.ARMY

CIOG6.ARMY.MIL

This page intentionally left blank.

Table of Contents

FOREWORD

The Army is already well on the way to achieving a secure, integrated, standards-based information environment. The Army network is evolving to eliminate redundancy and close security gaps by becoming inherently joint. We are leading the transition away from Service-centric approaches toward joint information technology acquisition, ownership and administration, and the delivery of end-to-end enterprise capabilities as described by the Joint Information Environment (JIE) construct. To achieve this end, the Army is implementing the Common Operating Environment (COE), which will enable secure and interoperable applications to be developed rapidly and used across a variety of computing environments.

LTG Robert S. Ferrell

The network will facilitate dissemination, analysis and storage of data. The volume, variety, rate of change and complexity of data today are impacting the Army's traditional information management practices. In order to succeed in today's information-driven environment, our data strategy needs to be at the heart of the Army's operating model and strategy.

The Army Data Strategy outlines the plan for implementing effective data management practices to improve situational awareness and decision making. To ensure that we enable success, one of my top priorities for network modernization, outlined in the Army Network Campaign Plan, is to develop strategy, policy and resources to deliver information technology (IT) services to the tactical edge. This Army Data Strategy supports this effort and serves as the overarching plan for achieving the Department of Defense Net-Centric Data Strategy's shared objective of making data, information and IT services visible, accessible, understandable, trusted and interoperable. The Army Data Strategy provides the plan for data producers and owners to maximize information availability to authorized consumers. This will allow commanders and their organizations to have broad and efficient access to data, reducing duplication of effort by leaders, Soldiers and their mission partners.

I applaud the work that has already been accomplished and challenge all Army organizations to embrace the goals and objectives outlined in this data strategy. Effective data management practices are essential to achieving the vision of a secure, integrated, standards-based environment that ensures uninterrupted global access and enables collaboration and decisive action throughout all operational phases across all environments. The Army Data Strategy will be critical to enabling the delivery of timely, trusted and shared information for the Army and our mission partners.

Robert S. Ferrell
Lieutenant General
Chief Information Officer/G-6

This page intentionally left blank.

EXECUTIVE SUMMARY

The Army Data Strategy describes the Army's vision and goals for establishing a solid foundation for sharing data, information and IT services across the Army – extending into the Joint Information Environment. The Army Data Strategy builds upon the Department of Defense (DoD) Net-Centric Data Strategy baseline of making data visible, accessible, understandable, trusted and interoperable. As part of these efforts, the Chief Information Officer/G-6 has partnered with the Assistant Secretary of the Army (Acquisition, Logistics and Technology) to implement the Common Operating Environment.

As an architectural paradigm, the Army network, which is the Army's portion of the DoD Information Network, is changing from a loose federation of stovepiped IT systems to a single, integrated, service-oriented, information-sharing environment. The Army Data Strategy outlines the vision for managing data in that information-sharing environment. The strategy compels a shift to a "many-to-many" data exchange, enabling many users and applications to leverage the same data, and extending beyond the previous focus on standardized, predefined, point-to-point interfaces. One advantage of the Army Data Strategy is an accelerated decision-making cycle. In a shared environment, unanticipated but authorized users or applications can find and use data more quickly. One of the CIO's goals is to populate the network (i.e., the NIPRNet, SIPRNet and JWICS[1]) with all data (intelligence and non-intelligence, raw and processed) to allow authorized users and applications access to this information without waiting for processing, exploitation and dissemination. All posted data will have associated metadata (i.e., data about data) to enable users and applications to discover and evaluate the utility of the data themselves and sharing the data.

The Army Data Strategy's collection of concepts, goals and initiatives are in various stages of maturity. They include the Army Information Architecture, which serves as a blueprint for developers and system owners by providing design and development guidance and a set of compliance requirements for assessing the level to which systems meet net-centric information-sharing objectives. It also includes the Army Authoritative Data Source process, which identifies an Army data asset recognized by a governing data authority as the single authoritative source for a particular kind of information. Information exchange specifications, which specify the physical format and the intended meaning of data that is exchanged between information systems, are also a key initiative of the Army Data Strategy. Data governance is a core objective of the Strategy as it provides an authoritative voice for the decisions and guidance provided to the data community.

As DoD moves toward a Joint Information Environment, the Army Data Strategy will enable strategic handling of data to produce secure and timely information exchange on the Army network anytime and anywhere. Implementation of the Army Data Strategy will provide three major benefits: 1) responsive discovery of, access to and integration of information; 2) effective decision-making through trusted information; and 3) protection and responsible sharing of information.

The Army Data Strategy will constantly evolve to ensure that the Army achieves its goals in an ever-changing technological landscape. The strategy will transform the way information is managed to accelerate decision making, improve joint warfighting and create intelligence advantages.

[1] NIPRNet is the Non-secure Internet Protocol Router Network. SIPRNet is the Secure Internet Protocol Router Network. JWICS is the Joint Worldwide Intelligence Communications System.

This page intentionally left blank.

1. INTRODUCTION

1.1 Purpose

The purpose of this document is to communicate the Army's vision and strategy for achieving a networked force enabled by data. The Army Data Strategy is a collection of concepts, goals and initiatives for managing data with the objective of making data, information and IT services visible, accessible, understandable, trusted and interoperable (VAUTI) throughout their life cycles for all authorized users when needed and regardless of location or access device. A good data strategy facilitates good decision making.

1.2 Scope

Achieving the vision will require proactive involvement in data management activities by everyone within the Army.

2. VISION

The Army Data Strategy seeks to enable Mission Command to gain a decisive operational advantage. The networked force requires the right data, at the right time, at the right place, limited only by policy and not by technology. This evolutionary approach focuses on the data rather than individual systems or communication networks.

3. GUIDING PRINCIPLES

The Army Data Strategy's guiding principles are high-level data guidance that apply to all aspects of system design and development. The principles below are further discussed in the Army Information Architecture.

3.1 Principle GA-01: Data are an enterprise asset. Information is enterprise currency. Knowledge is an enterprise resource.

3.2 Principle GA-02: Data are a physical representation of information but are not the same thing as information.[2]

3.3 Principle GA-03: Effective decision making and effective process execution in the Army require effective information sharing.

3.4 Principle GA-04: Information creators and managers have a responsibility and obligation to make their data visible and accessible to authorized consumers throughout the Army.

3.5 Principle GA-05: The information that drives decision making and Army processes is available to authorized consumers regardless of their location or the time of their request.

3.6 Principle GA-06: Compliance with Army governance and guidance documentation will enable, facilitate and promote effective information sharing among Army information systems and meet DoD information-sharing objectives.

3.7 Principle GA-07: The effectiveness of Army governance documentation can be measured (in part) by the cost savings that result from adopting the guidance/solutions.

[2] Data related to information technology.

3.8 Principle GA-08: Unclassified, sensitive or classified information must be handled according to law, regulation and policy to safeguard that data and information.

4. GOALS AND OBJECTIVES

The Army Data Strategy adopts, extends and refines the Department of Defense (DoD) Net-Centric Data Strategy (NCDS) and implementing instructions DoDI 8320.02 and DoDI 8320.07. By establishing repeatable and reusable processes and common technical standards for data exchange and data management, the Army will foster improved interoperability and quicker, more cost-efficient fielding of IT solutions, based on the *LandWarNet 2020 & Beyond Enterprise Architecture* for Mission Command.

The Army Data Strategy is critical to achieving the Common Operating Environment (COE). The COE establishes common communications and data standards that enable information sharing across the Joint Information Environment (JIE) and with mission partners. Wherever there is software running, there are data. Wherever there is persistent storage, there are data. The use of data by software is derivative of how data are represented and structured in those physical media. Data are either in persistent storage, in transmission or being processed in memory by software.

Given a resource-constrained environment and the greater emphasis on interoperability with our mission partners, compliance with the Army Data Strategy and architectural guidance is critical.

4.1 Strategic Goals and Enabling Objectives

The Army Data Strategy includes five goals. These goals, and the enabling objectives that refine and meet these goals, are presented in Table 1.

Army Strategic Goals	Enabling Objectives
Make Data Visible (V)	Post Data to Shared Spaces Register Metadata Related to Structure and Definition
Make Data Accessible (A)	Create Shared Spaces and Data Services (Also Information and IT Services) Associate Security-Related Metadata
Make Data Understandable (U)	Create Data Models Establish Data Integration Identify Information Requirements Traceability
Make Data Trusted (T)	Identify Authoritative Data Sources Create Secured Availability (Data Security and Data Access Security)
Make Data Interoperable (I)	Comply with Information Exchange Specifications Establish Master Data Management/Unique Identifiers Establish Community-Based Information Sharing Establish Translation and Mediation

Table 1 – Army Strategic Goals and Enabling Objectives

4.1.1 Make Data Visible

The goal of making data visible is to enable authorized users to discover authoritative data, information and IT services. The Data Services Layer - Army (DSL-A) is a framework and set of data service interface specifications that enable the Army and supporting organizations to develop data services that expose data assets, authoritative or otherwise, to consumers across the Army. DSL-A is similar to Content Discovery & Retrieval (CDR) Specifications (see Section 4.2.3.5).

4.1.1.1 Enabling Objective – Post Data to Shared Spaces

Users and applications will migrate from maintaining private data to making data available in community and enterprise shared spaces. These shared spaces will act as repositories, where users and applications can submit or post data assets to the enterprise. The shared spaces will provide storage and serving mechanisms. Enterprise shared spaces will be maintained, secured and staged as necessary to support the Army's missions. Data that are posted to shared spaces will be advertised via the associated metadata and will be discoverable with enterprise search tools.

4.1.1.2 Enabling Objective – Register Metadata Related to Structure and Definition

To facilitate discovery, users and applications will provide discovery metadata, in accordance with the DoD Discovery Metadata Standard (DDMS), for all data assets, particularly those posted to shared spaces. The DDMS will provide a common set of structured attributes that support discovery of data assets using search tools. The initial focus of the DDMS is to aid in the discovery of data assets as a whole; hence, the discovery metadata in the DDMS will not always be required for individual records or elements.

4.1.2 Make Data Accessible

The goal of making data accessible is to provide all credentialed consumers access to authoritative data, information and IT services via commonly supported access methods in accordance with law, policy and security controls (e.g., classification, need to know, compartmentalized controls, community of interest, etc.). It is the responsibility of the functional data owner to perform these actions for their authoritative data, information and IT services.

4.1.2.1 Enabling Objective – Create Shared Spaces and Data Services

Shared spaces – virtual and actual, such as enterprise data centers – will be created to provide a "store and serve" mechanism for data assets. Data access services are any mechanisms that help expose data that are not otherwise available to users and applications.

4.1.2.2 Enabling Objective – Associate Security-Related Metadata

Security-related metadata will be provided for each data asset as defined by the security descriptors element set within the core layer of the DDMS. Systems will control access in accordance with the asset's security-related metadata.

4.1.3 Make Data Understandable

The goal of making data understandable is to ensure that a data asset is usable by known and unanticipated authorized consumers through development and use of shared vocabularies.

4.1.3.1 Enabling Objective – Create Data Models

Data modeling encompasses procedures, methods, best practices, recommendations and subject matter expertise that support data model design, development and implementation. Data model guidance includes standardized, reusable schematic components for ubiquitous

concepts (e.g., person, location, time). These concepts establish common definitions of common terms, as well as their hierarchical relationships and ontologies, to define material domains with semantic precision. They can be incorporated into data models under development, vocabularies, taxonomies, data dictionaries and glossaries.

4.1.3.2 Enabling Objective – Establish Data Integration

Data integration is the process of combining data from two or more data assets and producing a single unified, consistent and cohesive view of the combined data. The objective is to create a set of data that represents the same information represented by the input data sets. Data integration may also refer to a data-centric strategy; an approach or architecture that is designed to support or implement an integrated, comprehensive, consistent, enterprise-spanning data deployment/management solution; and enterprise application interoperability.

4.1.3.3 Enabling Objective – Identify Information Requirements Traceability

Information requirements will describe the information needed to drive enterprise processes and capabilities. Information requirement traceability will ensure that the right information is available and can be supplied to the right end users in the Army and among mission partners.

4.1.4 Make Data Trusted

The goal of making data trusted consists of the following: ensure secure access; establish known pedigree and security level of data; and provide information from an approved authoritative source.

4.1.4.1 Enabling Objective – Identify Authoritative Data Sources (ADS)

ADS enable commanders, decisions makers and all Army personnel access to Army-certified (accurate, timely and high-quality) internal and external data sources containing trusted information. Reuse of registered ADS is key to improving mission effectiveness through system interoperability and to reducing the time, effort and resources required to operationally integrate Army systems.

4.1.4.2 Enabling Objective – Create Secured Availability (Data Security and Data Access Security)

Secured availability involves protecting the confidentiality, integrity and availability of Army information. Secured availability will provide systemic security mechanisms that are an integral part of system design, development, fielding and operations.

4.1.5 Make Data Interoperable

The goal of making data interoperable is for data providers to utilize non-proprietary, open source, industry or DoD-designated standards to ensure that data are useable across multiple systems and applications.

4.1.5.1 Enabling Objective – Comply with Information Exchange Specifications (IESs)

Reuse of IESs is key to improving the effectiveness of system interoperability and reducing the time, effort and resources required to operationally integrate Army systems.

4.1.5.2 Enabling Objective – Establish Master Data Management and Unique Identifiers

Master data management will provide a set of processes and tools that ensure that master data are effectively controlled, updated and used within and throughout enterprise software systems. Master data are typically shared and used by different software applications across the enterprise, often as part of transaction processing. Master data provide a continuity and consistency of knowledge throughout the enterprise, and are routinely used in many existing

technologies, such as data warehouses, data quality, data integration and data mapping and translation. Unique identifiers are a form of master data that enable interoperability and consistency of data assets across the Army enterprise.

4.1.5.3 Enabling Objective – Establish Community Based Information Sharing

Interoperability communities may provide an informal, loosely organized group of members or a formal group that is organized as a community of interest, where a member is a system, service, application or data asset that is coupled with a human representative. An interoperability community can be described as a community of members that share information frequently in collaborative pursuit of a mission. The format and meaning of data exchanged with entities outside the community are the collective responsibility of the community. This can be best accomplished through the use of industry standards.

4.1.5.4 Enabling Objective – Establish Translation and Mediation

Translation and mediation will provide a mechanism where data are translated from their original schematic format to a schematic format more suitable for the receiver through a mediating agent. Mediation involves a “third party” neutral mediating format (e.g., one governed by an IES) that acts as an intermediary between the sender and receiver. Translations are involved in the exchange of data when a mediating form is used. Mediation may involve a sequence of transformation or translation stages. Use of translation and mediation should be minimized as much as practical; industry standards can be effective in reducing the need for them.

4.2 Relationship to Common Operating Environment (COE) and the Army Network

The Army Data Strategy is aligned to and complements the JIE, COE Architecture, Army Identity and Access Management Reference Architecture Version 4.0 and the LandWarNet 2020 End-State Army Enterprise Architecture. The implementing guidance discussed in Section 4.2 complements the COE Implementation Plan and is reflected in COE cross-cutting capabilities. Central to the Army network are data and enterprise services that are specifically related to discovering, accessing and managing data/information. The Army Data Strategy provides the foundation for and implements these services.

4.3. Challenges and Mitigations

Army systems and applications depend on shared data. The Army Data Strategy is designed to foster an environment where data are readily accessible and available to all authorized users, applications and systems. Although implementing the Army Data Strategy will make data available to a certain degree, challenges will remain. The table below lists the obvious challenges, along with recommended mitigation. More complicated challenges and issues may be addressed by the Army data governance process.

Challenges	Mitigations
Visible – Some data stewards choose not to register their Authoritative Data Sources and associated metadata, thereby creating data silos.	Enforce compliance with current DoD Instructions and Army guidance regarding the registration of ADSs and creating associated metadata, including discovery metadata, for each asset.
Accessible – Web services that allow access to exposed data do not exist.	Develop and publish web services for all authoritative data sets throughout the enterprise.
Understandable – Lack of data standardization.	Develop a data element guide and vocabulary registry, populated with a set of common elements.
Trusted – (1) Inconsistent, incomplete or lack of Identity and Access Management (IdAM) solution. (2) Trusted information is difficult to achieve. (3) Lack of standardized data at rest (DAR).	(1) Incorporate enterprise-level IdAM solution to protect trusted environments. (2) To help ease the difficulty of producing trusted information, effective metadata tagging principles should be employed. (3) Standardize DAR.
Interoperable – Non-compliant standard for or lack of Information Exchange Specifications (IESs) in developed information systems.	Incorporate industry standard IESs.

Table 2 – Challenges and Mitigations of the Strategic Goals of the Army Data Strategy.

5. IMPLEMENTATION GUIDANCE AND THE ARMY DATA MANAGEMENT PROGRAM (ADMP)

The implementation guidance provided via the Army Data Management Program (ADMP) is the primary expression of and instrument for executing the Army Data Strategy. Figure 1 portrays DoD and Army influencing guidance for the ADMP, implementing guidance products developed under the ADMP, governance of the ADMP and the transition from guidance to implementation. Mission Command success requires that the ADMP guidance be integrated into the Common Operating Environment and the operational environment.

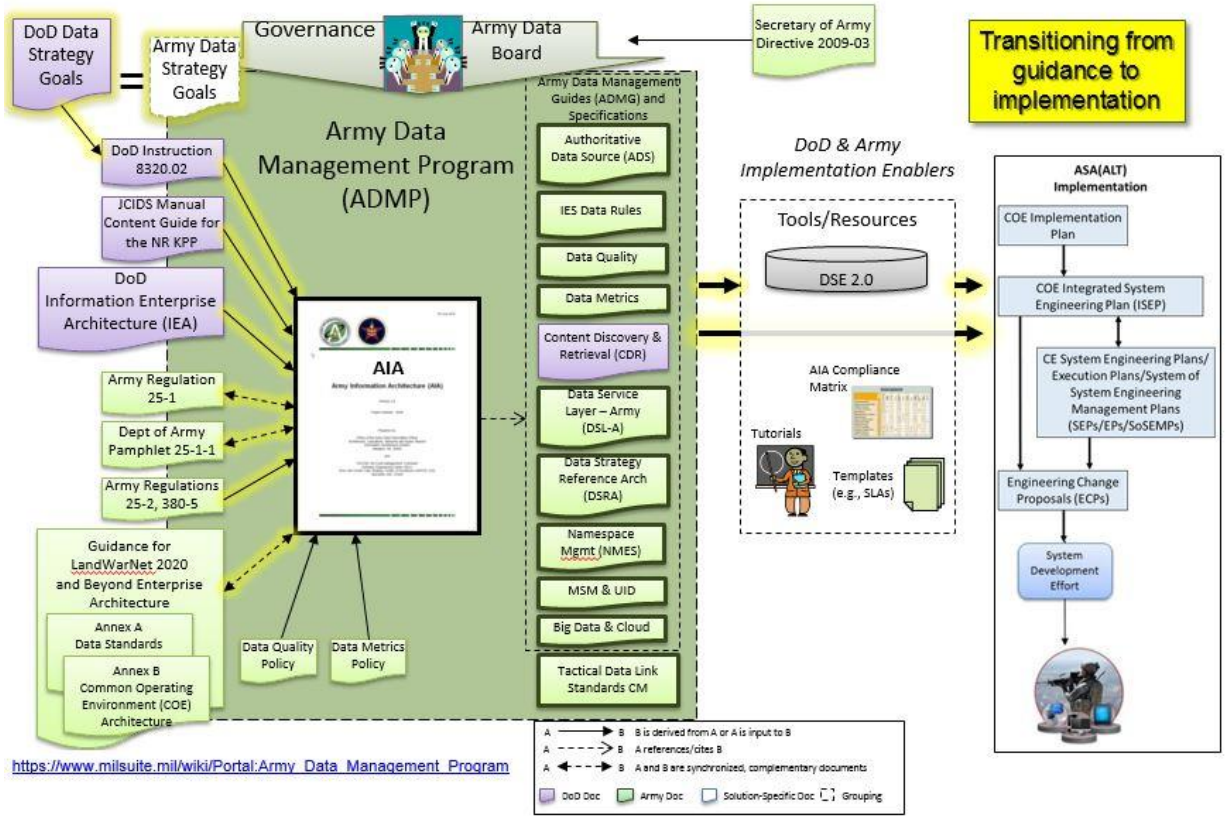

Figure 1 – Army Data Management Program

5.1 Army Data Governance

Army Directive 2009-03*, Army Data Management*, created the **Chief Data Officer** (CDO) position, the **Army data steward** role and the **Army Data Board** (ADB). The Army Data Council and functional data managers were established by the Army Data Board Charter. The Army Data Board and Army Data Council foster a collaborative governance environment for achieving Army Data Strategy goals, with active participation from across the Army.

5.2 Army Information Architecture (AIA)

The centerpiece of the ADMP is the **Army Information Architecture (AIA)**. The AIA translates DoD and Army guidance into actionable and measureable rules to guide material development and operational practices. The AIA provides the foundation to enable the transformation to mission-responsive information sharing in two ways. The first is as design and development guidance for enabling information sharing; the second is as a set of compliance requirements for assessing the level to which systems meet the DoD and Army mission-responsive information-sharing objectives.

The primary content of the AIA is a collection of principles and business rules that are organized around and address the following topics: data asset development and management; data and services deployment; data delivery and use; and secured availability. The AIA is based on the concepts and principles from the internationally recognized Data Management Association (DAMA). The Army-tailored version of the Data Management Body of Knowledge (DMBOK) wheel (see Figure 2) displays concentric rings that expand from governance at the center to core, pervasive data management functions to operational, implementable data management functions to special topics that enable the Army to effectively and efficiently carry out its

missions. Each outer ring depends on functions and capabilities identified by the inner rings. Each ring should be regarded as a rotating wheel with no implied alignment to its outer ring. Data standards underlie all functions and topics.

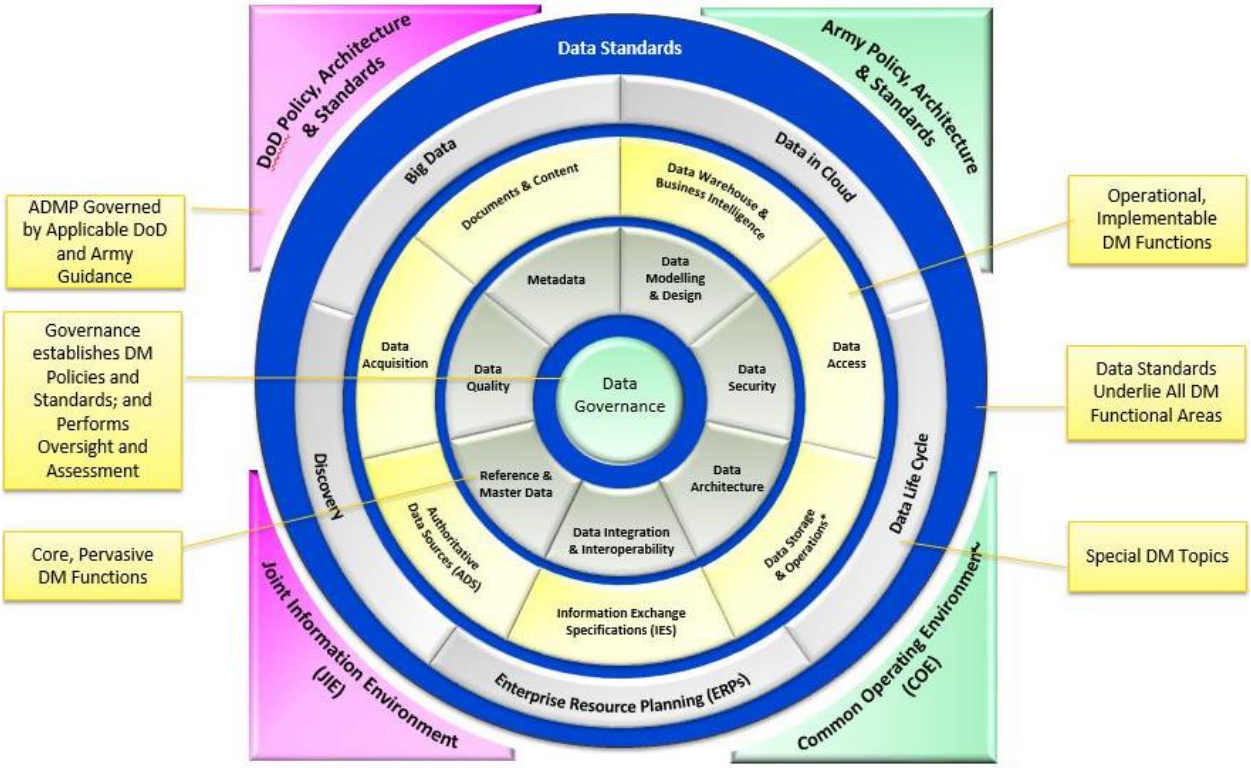

Figure 2 – ADMP Wheel depicting data management functions as they relate to fulfillment of the goals of the Army Data Strategy.[3]

5.3 Army Data Management Program Guides and Specifications

The Army Data Management Guides (ADMGs) are a suite of reference documents that provides detailed guidance for selected topics introduced in the AIA. Each topic area guide defines the subject topic and presents an implementation framework and the standards and technology that support the framework. In addition, best practices, business benefits and governance guidance supporting the topic area are included. The ADMGs align with DoD and Army mission-responsive and architecture policies and guidance, specifically DoD Instruction 8320-02, *Sharing Data, Information and Information Technology (IT) Services in the DoD*, the DoD Information Enterprise Architecture (DIEA), the Army Information Architecture and the Definitions and Guidance for the Common Operating Environment: Annex B to LandWarNet

[3] The Army Data Management Program (ADMP) defines the Army Data Management (ADM) Framework (also known informally as the "ADMP Wheel"). The ADM Framework is based on and extends the DAMA Data Management Body of Knowledge (DMBOK) Functional Area Framework (also known as the "DAMA Wheel"). DAMA is a reputable international association of data management professionals that develops and provides resources (such as the DMBOK) to support data management professionals worldwide. The ADM Framework directly adopts the DMBOK functional areas as the core, the central ring and some segments of the middle ring. The framework augments the DAMA functional areas by adding functional areas of particular importance to the Army, such as ADSs and IESs, to the middle and outmost ring. The segments of the ADM Framework represent operational and implementable data management functions, as well as special data management topics. The rings and their segments are underpinned by data standards. The principles and guidance provided by the ADMP within the ADM Framework are based on and aligned with Army and DoD policy, architecture and standards; the Army Common Operating Environment; and the DoD Joint Information Environment.

2020 and Beyond Enterprise Architecture. The combination of these guides and specifications enables a more effective information-sharing environment that promotes the key data aspects of visibility, accessibility, understandability, trust and interoperability. Additional ADMGs are forthcoming.

5.3.1 Army Data Management Guides

5.3.1.1 Data Quality Management

All Army organizations producing or maintaining enterprise data must incorporate a comprehensive data quality management program (DQMP) as part of their data production and maintenance activities. As described in Army Regulation 25-1 and the ADMG for data quality management, the DQMP comprises the policies and procedures for selecting and implementing data-quality standards in order to ensure that Army information products achieve and maintain the required level of data quality necessary to support all Army enterprise-wide operations and processes. The primary objectives of DQMP are to provide quality data to the users and systems that need it, and to reduce the IT and operational inefficiencies within the Army. The DQMP is essential to meeting DoD Net-Centric Data Strategy goals.

5.3.1.2 Army Data Strategy Metrics

The primary objective of the Data Strategy Metrics (DSM) Guide is to identify the important characteristics of data management capabilities needed to meet Army Data Strategy goals and objectives; and to establish ways to measure how well the organization is providing these capabilities. DSM allow the Army to determine its current level of data management capabilities and to evaluate improvement over time.

5.3.1.3 Master Data Management (MDM) and Unique Identifiers

Master data are the consistent and uniform set of identifiers and extended attributes that describe the core entities of an enterprise (non-transactional data entities), and are used across multiple business processes. The MDM Guide is a set of disciplines, processes and technologies for ensuring the accuracy, completeness, timeliness and consistency of multiple domains of enterprise data across applications, systems and databases, and across multiple business processes, functional areas, organizations, geographies and channels.

As stated in DoD Directive 8320.03, *Unique Identification (UID) Standards for a Net-Centric Department of Defense*, UIDs are a technology-independent mechanism that support integration and interoperability by providing an enterprise-wide common ID for significant Army assets. This ID is used to link and integrate data about that asset into other data assets. All Army data collected and maintained in data assets designated to support Army enterprise capabilities will use globally unique identification to ensure full data integration, referential integrity and data interoperability. Unique identifiers for discrete entities, their associated attributes and their relationships shall be explicit throughout the Army enterprise and will enable data discovery, correlation and sharing of information between users in a mission-responsive environment.

5.3.1.4 Big Data Management for Decision Analytics and Cloud Computing

“Big Data” is a term that describes very large, rapidly changing and differently structured data sets that are impractical to manage using conventional data processing techniques. Big Data are often said to have the following characteristics: volume (very large), velocity (rapidly changing) and variety (differently structured). Big Data “data stores” may consist of structured and unstructured data. The primary uses of Big Data are analytics, attribution and algorithms.

The Army will utilize a two-pronged approach for managing Big Data. First, the Army will re-double its efforts to implement effective data management methodologies to ensure that data

are authoritative, timely, secure and of the highest quality. Second, the Army will develop a process for the identification, development and implementation of efficient decision support and analytical tools to best maximize the use of information derived from Big Data extrapolation. The Army will leverage the unprecedented growth of data and data sources to support better-informed decision making and create higher-value information by "connecting the dots" across a myriad of large data sets. The Army's Big Data effort should provide good quality data, technical guidance and policy mechanisms for more responsive, informed and precise support to military and defense operations (see Figure 3).

5.3.2 Army Data Management Specifications

5.3.2.1 Authoritative Data Source (ADS)

ADSs are recognized or official data production sources with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers. An ADS may be the functional combination of multiple, separate data sources. The DoD enterprise capability, known as the Data Services Environment, provides centralized access to authoritative data sources to improve search, access, consistency and integration of data services, as well as to increase collaboration amongst data producers and consumers. As more ADSs are registered and their data assets are web-service accessible, the ADS registration will be accompanied with registration and association of active web services, web service descriptions and the IESs that are implemented via the web services. The developer can quickly identify relevant data sources and also see the methods that are available to access the data directly, thereby fostering more agile capability development. The ADS Process describes the ADS registration process.

5.3.2.2 Information Exchange Specification (IES) Data Rules

To enable interoperability, information exchanges among new and upgraded capabilities in Army IT systems must conform to industry standard IESs or be approved exceptions. An IES is a set of materials that specifies how data are to be exchanged between software applications. An IES defines a particular data exchange and explains what developers must know to write code that produces or consumes an instance of that exchange. At a minimum, an IES specifies at least one schema that governs the physical data format for the exchanged data, a glossary that defines the schema elements and the relationships among them, and the definition of extra-schema constraints governing the validity of data that conform to the schema. The rules for cross-cutting capability (CCC) IESs in interface specifications (known informally as the IES Data Rules) specify requirements governing the use of particular CCC IESs to exchange data between systems. The interface specifications support the interoperability of systems/services providing cross-cutting capabilities.

The National Information Exchange Model (NIEM) is a standardized IES framework for the development of eXtensible Markup Language-based machine-to-machine data exchanges. The NIEM framework specifies rules and predefined data components for creating an IES. NIEM adoption and implementation must be planned and resourced in a responsible manner. All Army developers should consider NIEM in accordance with the DoD NIEM First memorandum, which states, "DoD organizations shall first consider NIEM for their information-sharing solutions when deciding which data exchange standards or specifications meet their mission and operational needs." In cases where the program manager (PM) does not implement NIEM, the PM is responsible for submitting an exception waiver request to the component acquisition executive.

5.3.2.3 Content Discovery & Retrieval (CDR)

The Army is adopting the CDR Reference Architecture, Specification Framework and Service Specifications jointly developed by the DoD and Intelligence Community to define a common, brokered, federated, search architecture. CDR components are DoD standards, registered in the Defense Information Systems Repository (DISR) and implemented by DoD's managed service provider for enterprise search.

5.3.2.4 Data Service Layer-Army (DSL-A)

The DSL-A Guide is a service-oriented architecture framework that specifies a set of data service interfaces to make Army data available to consumers across the Army. The DSL-A adopts and builds on CDR specifications to enable Army system designers, developers and supporting organizations to create standardized data services that expose data sources and, thus, meet the data accessibility goal.

5.3.2.5 Data Strategy Reference Architecture (DSRA)

The DSRA Guide is a comprehensive set of architectural views based upon the Army Data Reference Model (DRM) and the "bricks and patterns" methodology: a set of reusable components (bricks) and combinations or configurations of those components that are repeated in separate implementations (patterns).

5.3.2.6 Namespace Management Enterprise Solution (NMES)

The NMES provides a solution for namespace management at the Army enterprise level, including naming and governance. The NMES provides the capabilities necessary to label, register, govern, manage and resolve collisions between or among the set of namespaces that meet the criteria of interest.

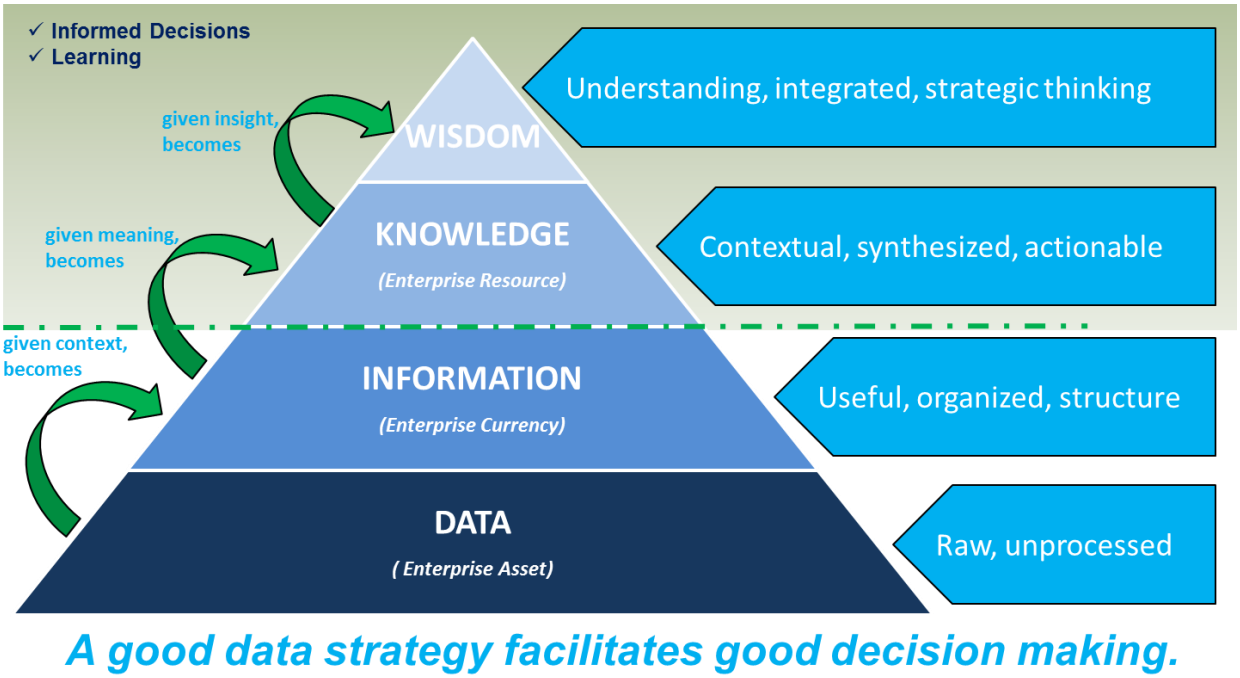

Figure 3 – Making Informed Decisions

The Army recognizes that not every data requirement will require a Big Data solution. The Army also recognizes that there are quality and integrity issues, as well as gaps in Army data. In some cases, data stewards are unwilling or unable to share data for various reasons. These challenges can impact any Big Data project.

The Cloud Computing Guide explains how the Army can use cloud technology to achieve the goals outlined in the DoD Strategic Plan, and complements the Army Cloud Computing Strategy. Cloud computing incorporates service-oriented architecture standards and technology to make data visible, accessible and understandable, and includes additional capabilities to make data more reliable and secure.

5.3.3 Operational/Tactical Data Link Standards Configuration Management

To ensure seamless interoperability, Army systems that send or receive data-link or character-oriented messages must comply with jointly approved military standards, to include the Joint Interoperability of Tactical Command and Control Systems family of standards and any appropriate NATO standardization agreements when operating in a NATO environment. The Army coordinates positions and recommends changes to these standards through the Army Configuration Control Board (CCB). The CCB coordinates Army positions through Joint governance bodies and some mission partners, then aligns and harmonizes them with NATO, as well as separately with other allied non-NATO nations. Joint coordination is provided by the Joint Multi-Tactical Data Link Standards Working Group, the Joint Multi-Tactical Data Link Configuration Control Board, the U.S. Message Text Format Configuration Control Board and the Joint Combat Net Radio Working Group.

5.3.4 Mobility Strategy

The Mobility Strategy relies on authorized users, transport mechanisms, data and authentication to ensure the level of trust required to access applications and display information on request. The Army Data Strategy ensures that data are accessible and provides a foundation for use on the end-user (mobile) device. The Army Mobility Strategy and the Army Data Strategy will align with the Army Cloud Computing Strategy to ensure access to data for the user anytime, anyplace, regardless of device. While the Army Mobility Strategy matures, as an alternative, mobility concepts and a framework can be found in the DoD Mobility Strategy.

6. ROLES AND RESPONSIBILITIES

6.1 Army Chief Information Officer (CIO)/G-6

The Army CIO/G-6 is responsible for Army information management at the strategic level. The CIO/G-6 will establish and oversee the Army Data Management Program and appoint a Chief Data Officer in accordance with Army Directive 2009-03.

6.2 Second Army

Second Army, in coordination with Army Cyber Command (ARCYBER), will prescribe the operational aspects of information protection and data security, including processes that enforce Army-wide compliance with the Federal Information Security Management Act of 2002 and Office of Management and Budget Circular A-130. ARCYBER also will identify and analyze threats to the Army global enterprise network and its enabling technologies.

6.3 Chief Data Officer (CDO)

The CDO is responsible for developing and implementing the Army Data Management Program. The CDO is the senior advisor to the Secretary of the Army and the Chief of Staff of the Army

on data issues. The CDO also chairs the Army Data Board; oversees the development and execution of the Army Data Strategy; and provides governance that underpins and supports all Army Data initiatives. The CDO oversees the activities of the Army Data Council.

6.4 Army Data Board (ADB)

The Army Data Board serves as the senior Army enterprise data decision body. The ADB develops coordinated Army enterprise positions on data strategy, standards and execution; serves as the senior adjudication body for Army enterprise data issues; coordinates data-sharing efforts across the Army enterprise; serves as the certification and waiver approval authority for targeted standards as delegated by the CDO; and collects and disseminates best practices and lessons learned for the data community.[4]

6.5 Army Data Stewards

Data stewards are subject matter experts in their area's operational requirements and processes. Under the direction of the CDO, data stewards are responsible for enforcing federal, Army and their organization's data standards, processes and procedures. Army data stewards serve as voting members of the Army Data Board.

6.6 Army Data Council

The Army Data Council serves as the Army Data Board's initial adjudication forum for data topics and the development and implementation of the Army Data Strategy.

6.7 Functional Data Manager (FDM)

FDMs establish, manage and/or participate in data governance bodies for their area of responsibility that manage and execute the Army Data Management Program, Army Data Strategy and Army Information Architecture; and oversee the harmonization and adjudication process, raising any unresolved issues to the Army Data Board.

7. CONCLUSION

As DoD moves toward a Joint Information Environment and the Intelligence Community moves toward an Intelligence Community Information Technology Environment, strategic handling of data will enable secure information exchange on the Army network anytime and anywhere.

The Army Data Strategy does not apply to a specific technology. Rather, it takes a cross-enterprise architectural perspective that connects how data are stored, how they are moved across network architectures and how they provide the information needed by warfighters, commanders and all authorized consumers across the Army, DoD, Mission Partner Environment and Intelligence Community Information Technology Environment.

The data strategy describes a path forward to realize Army and DoD data, information and IT services objectives, providing data management planning and implementation guidance to Army data stewards, data owners and data producers to maximize the sharing of Army data, information and IT services. This will enable commanders, their organizations and our mission partners to have broad, efficient and timely access to authoritative data. The strategy also provides the roadmap to increase interoperability among systems and reduce development and sustainment costs. The Army Data Strategy is being implemented through the Common Operating Environment and numerous ongoing operational data efforts across the Army.

[4] Army Data Board Charter, version 5.023, dated 14 July 2014

Additional detailed guidance is provided in the Army Data Management Program, the Army Information Architecture and the Army Data Management Guides.

Appendix A: References

[1] DoD Instruction 8320.02, Sharing Data, Information and Information Technology (IT) in the Department of Defense, 5 August 2013. http://dtic.mil/whs/directives/corres/pdf/832002p.pdf

[2] DoD Directive 8320.03, Unique Identification (UID) Standards for a Net-Centric Department of Defense, 23 March 2007. http://dtic.mil/whs/directives/corres/pdf/832003p.pdf

[3] Memorandum, DoD Chief Information Officer, 9 May 2003, subject: DoD Net-Centric Data Strategy. http://dodcio.defense.gov/Portals/0/Documents/Net-Centric-Data-Strategy-2003-05-092.pdf

[4] DoD Instruction 8320.07, Implementing the Sharing of Data, Information, and Information Technology (IT) Services in the Department of Defense, 3 August 2015. http://www.dtic.mil/whs/directives/corres/pdf/832007p.pdf

[5] Memorandum, DoD Chief Information Officer, 10 August 2012, subject: DoD Information Enterprise Architecture 2.0. http://dodcio.defense.gov/Portals/0/Documents/DIEA/DoD%20IEA%20v2.0_Volume%20I_Description%20Document_Final_20120730.pdf

[6] Department of Defense Data Services Environment (DSE). https://metadata.ces.mil/

[7] Department of Defense Discovery Metadata Specification (DDMS), Version 4.1, 12 June 2012. http://metadata.ces.mil/dse/irs/DDMS/DDMS_4_1_overview.html

[8] Army Directive 2009-03, Army Data Management, 30 October 2009. http://armypubs.army.mil/epubs/pdf/ad2009_03.pdf

[9] Army Regulation 25-1, Army Information Technology, 25 June 2013. http://www.apd.army.mil/pdffiles/r25_1.pdf

[10] Joint Information Environment (JIE). https://intelshare.intelink.gov/sites/jie/

[11] DoD Instruction 8110.01, Mission Partner Environment (MPE) Information-Sharing Capability Implementation for the DoD, 25 November 2014. http://www.dtic.mil/whs/directives/corres/pdf/811001p.pdf

[12] Intelligence Community Information Technology Enterprise (IC ITE). http://www.dni.gov/ICEA/default.htm

[13] LandWarNet 2020 and Beyond Enterprise Architecture, 15 August 2014. http://ciog6.army.mil/Portals/1/Architecture/2014/20140801-LWN_2020_EA_V2-0.pdf

[14] Definitions and Guidance for the Common Operating Environment: Annex B to LandWarNet 2020 and Beyond Enterprise Architecture. http://ciog6.army.mil/Portals/1/Architecture/2014/20140801-Annex_B_Definitions_Guidance_COE_V2-0.pdf

[15] Army Data Management Program (ADMP). https://www.milsuite.mil/wiki/Portal:Army_Data_Management_Program

[16] Army Information Architecture (AIA), 5 June 2013.
http://ciog6.army.mil/Portals/1/Architecture/ArmyInformationArchitecturev4-1dtd2013-06-05.pdf

[17] Army Data Board Charter, version 5.023, 14 July 2014.
https://www.intelink.gov/go/1dREQNg

[18] Army Data Management Guides.
https://www.milsuite.mil/wiki/Portal:Army_Data_Management_Program/ADF

[19] Data Management Association: Data Management Body of Knowledge (DMBOK).
http://www.dama-dmbok.org/

[20] Authoritative Data Sources Process.
https://www.milsuite.mil/wiki/Authoritative_Data_Sources_Process

[21] Rules for Cross-Cutting Capability Information Exchange Specifications in Interface Specifications. https://www.milsuite.mil/wiki/IES_Data_Rules

[22] Memorandum, DoD Chief Information Officer, 28 March 2013, subject: Adoption of the National Information Exchange Model within the Department of Defense.
http://dodcio.defense.gov/Portals/0/Documents/2013-03-28%20Adoption%20of%20the%20NIEM%20within%20the%20DoD.pdf

[23] Data Quality Management Guide. https://www.milsuite.mil/wiki/ADF_-_Data_Quality_Management

[24] Data Strategy Metrics Guide. https://www.milsuite.mil/wiki/ADF_-_Data_Strategy_Metrics

[25] Content Discovery and Retrieval Architecture Products.
https://www.intelink.gov/wiki/CDRIPT

[26] Data Services Layer-Army. https://www.milsuite.mil/wiki/Data_Services_Layer-Army

[27] Data Strategy Reference Architecture.
https://www.milsuite.mil/wiki/Data_Strategy_Reference_Architecture

[28] Namespace Management Enterprise Solutions.
https://www.milsuite.mil/wiki/Namespace_Management_Enterprise_Solution_(NMES)

[29] Data Aspects of Cloud Computing Guide. https://www.milsuite.mil/wiki/ADF_-_Data_Aspects_of_Cloud_Computing

[30] Unique Identification. https://www.milsuite.mil/wiki/UID

[31] Army Cloud Computing Strategy.
http://ciog6.army.mil/Portals/1/20150424_Army_Cloud_Computing_Strategy.pdf

[32] NIST Special Publication 1500-1, Draft NIST Big Data Interoperability Framework, Volume 1, Definitions, 6 April 2015. http://bigdatawg.nist.gov/_uploadfiles/M0392_v1_3022325181.pdf

[33] DoD Mobile Device Strategy, 8 June 2012.
http://oai.dtic.mil/oai/oai?verb=getRecord&metadataPrefix=html&identifier=ADA560434

[34] Identity and Access Management (IdAM) Version 4.0.
http://ciog6.army.mil/Architecture/tabid/146/Default.aspx

[35] Mission Command White Paper, 3 April 2012.
http://www.dtic.mil/doctrine/concepts/white_papers/cjcs_wp_missioncommand.pdf

Appendix B: Acronyms and Definitions

Acronyms

ADB	Army Data Board
ADM	Army Data Management
ADMG	Army Data Management Guides
ADMP	Army Data Management Program
ADS	Authoritative Data Source
AIA	Army Information Architecture
ANCP	Army Network Campaign Plan
ARCYBER	Army Cyber Command
ASA(ALT)	Assistant Secretary of the Army (Acquisition, Logistics and Technology)
CCB	Configuration Control Board
CCC	Cross-Cutting Capability
CDO	Chief Data Officer
CDR	Content Discovery & Retrieval
CIO/G-6	Army Chief Information Officer/G-6
COE	Common Operating Environment
DAMA	Data Management Association
DAR	Data at Rest
DDMS	DoD Discovery Metadata Standard
DIEA	DoD Information Enterprise Architecture
DISR	Defense Information Systems Repository
DMBOK	Data Management Body of Knowledge
DoD	Department of Defense
DoDIN	DoD Information Network
DQMP	Data Quality Management Program
DRM	Data Reference Model
DSE	Data Services Environment
DSL-A	Data Services Layer – Army
DSM	Data Strategy Metrics
DSRA	Data Strategy Reference Architecture
FDM	Functional Data Manager
IdAM	Identity and Access Management
IES	Information Exchange Specifications
IP	Internet Protocol
IT	Information Technology
JIE	Joint Information Environment
JWICS	Joint Worldwide Intelligence Communications System
NCDS	Net-Centric Data Strategy
MDM	Master Data Management
MPE	Mission Partner Environment
NCDS	Net-Centric Data Strategy
NIEM	National Information Exchange Model
NIPRNet	Non-classified Internet Protocol (IP) Router Network
NMES	Namespace Management Enterprise Solution
PM	Program Manager
SIPRNet	Secret Internet Protocol Router Network
UID	Unique Identification
VAUTI	Visible, Accessible, Understandable, Trusted and Interoperable

Definitions

Shared spaces: A mechanism that provides storage of and access to data for users within a bounded network space. Enterprise shared space refers to a store of data that is accessible by all users within or across security domains on the DoD Information Network. A shared space provides virtual or physical access to any number of data assets (e.g., catalogs, websites, registries, document storage and databases). As described in this strategy, any user, system or application that posts data uses shared space. This definition is taken from the DoD Net-Centric Data Strategy, dated 9 May 2003.

Metadata: "Data about data." There are two types of metadata: *structural metadata* and *descriptive metadata*. Structural metadata are data about the containers of data. Descriptive metadata use individual instances of application data or the data content.

This page intentionally left blank.

In memory of Mr. Cliff Daus, former Division Chief of the Army Chief Information Office/G-6's Data Management Division. Cliff Daus led the U.S. Army's first-ever effort to create a Data Strategy.

Completing the Data Strategy was his last official accomplishment and culminated a lifetime of public service. He was a tremendous Soldier, an exemplary Army Civilian, and most importantly, a wonderful husband, father and friend to so many.

May he rest in peace.