Downloaded from http://www.everyspec.com

Department of Defense
DIRECTIVE

NUMBER 8320.2
December 2, 2004

ASD(NII)/DoD CIO

SUBJECT: Data Sharing in a Net-Centric Department of Defense

References: (a) DoD Directive 8320.1, "DoD Data Administration," September 26, 1991 (hereby canceled)
(b) Department of Defense Chief Information Officer Memorandum, "DoD Net-Centric Data Strategy," May 9, 2003
(c) DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002
(d) Department of Defense Discovery Metadata Specification[1]
(e) Deputy Secretary of Defense Memorandum, "Information Technology Portfolio Management," March 22, 2004
(f) Director of Central Intelligence Directive 8/1, "Intelligence Community Policy on Intelligence Information Sharing," June 9, 2004 (U//FOUO)

1. PURPOSE

This Directive:

1.1. Cancels reference (a) and establishes policies and responsibilities to implement data sharing, in accordance with reference (b), throughout the Department of Defense.

1.2. Directs the use of resources to implement data sharing among information capabilities, services, processes, and personnel interconnected within the Global Information Grid (GIG), as defined in reference (c).

1.3. Authorizes the publication of DoD issuances consistent with the policies herein and in reference (b).

[1] Latest version available at DoD Metadata Registry (http://diides.ncr.disa.mil/mdregHomePage/mdregHome.portal)

Downloaded from http://www.everyspec.com

2. APPLICABILITY AND SCOPE

This Directive applies to:

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

2.2. All data assets and information that are or may be available within the GIG.

3. DEFINITIONS

Terms used in this Directive are defined in enclosure 1.

4. POLICY

It is DoD policy that:

4.1. Data is an essential enabler of network-centric warfare (NCW) and shall be made visible, accessible, and understandable to any potential user in the Department of Defense as early as possible in the life cycle to support mission objectives.

4.2. Data assets shall be made visible by creating and associating metadata ("tagging"), including discovery metadata, for each asset. Discovery metadata shall conform to the Department of Defense Discovery Metadata Specification (reference (d)). DoD metadata standards shall comply with applicable national and international consensus standards for metadata exchange whenever possible. All metadata shall be discoverable, searchable, and retrievable using DoD-wide capabilities.

4.3. Data assets shall be made accessible by making data available in shared spaces. All data assets shall be accessible to all users in the Department of Defense except where limited by law, policy, or security classification. Data that is accessible to all users in the Department of Defense shall conform to DoD-specified data publication methods that are consistent with GIG enterprise and user technologies.

4.4. Data assets shall be made understandable by publishing associated semantic and structural metadata in a federated DoD metadata registry.

4.5. To enable trust, data assets shall have associated information assurance and security metadata, and an authoritative source for the data shall be identified when appropriate.

Downloaded from http://www.everyspec.com

4.6. Data interoperability shall be supported by making data assets understandable and by enabling business and mission processes to be reused where possible.

4.7. Semantic and structural agreements for data sharing shall be promoted through communities (e.g., communities of interest (COIs)), consisting of data users (producers and consumers) and system developers, in accordance with reference (b).

4.8. Data sharing concepts and practices shall be incorporated into education and awareness training and appropriate DoD processes.

5. RESPONSIBILITIES

5.1. The Assistant Secretary of Defense For Networks and Information Integration/ Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) shall:

5.1.1. Guide and oversee matters relating to Net-Centric data sharing in support of the DoD Components, COIs, Domains, and Mission Areas by:

5.1.1.1. Developing, maintaining, and enforcing enterprise metadata direction that uses existing Government and industry metadata standards when possible.

5.1.1.2. Developing and maintaining direction on, and enabling use of, federated enterprise capabilities to publish metadata and to locate, search, and retrieve metadata and data. Federated enterprise capabilities shall include the Intelligence Community (IC).

5.1.1.3. Develop the policies and procedures to protect Net-Centric data while enabling data sharing across security domains and with multi-national partners, other Federal Agencies, and State and local governments in accordance with law, policy, and security classification, in coordination with the Under Secretary of Defense For Intelligence (USD(I)) and the Under Secretary of Defense For Policy (USD(P)).

5.1.2. In accordance with the Deputy Secretary of Defense Memorandum (reference (e)), ensure that Domains within the Enterprise Information Environment Mission Area promote Net-Centric data sharing and effectively enable COIs, including adjudicating conflicts in metadata agreements and identifying authoritative sources.

5.1.3. As an element of Information Technology (IT) portfolio reviews, and in accordance with reference (e), provide guidance to evaluate and measure:

5.1.3.1. The status of the DoD Components in achieving Net-Centric data sharing.

5.1.3.2. The degree to which Mission Area and Domain portfolios provide the capabilities needed to share data.

Downloaded from http://www.everyspec.com

5.2. The Under Secretary of Defense for Acquisition, Technology, and Logistics, in coordination with the ASD(NII)/DoD CIO, shall:

5.2.1. Ensure that the Defense Acquisition Management System policies and procedures incorporate the policies herein, and provide guidance for Milestone Decision Authorities to evaluate and approve system or program satisfaction of data sharing practices, in accordance with reference (e).

5.2.2. Ensure that the Defense Acquisition University develops education and training programs to advocate Net-Centric data sharing in the Department of Defense based on policies herein.

5.3. The Under Secretary of Defense For Policy shall collaborate with the ASD(NII)/DoD CIO and the USD(I) to develop the policies and procedures to protect Net-Centric data while enabling data sharing across different security classifications and with multi-national partners, other Federal Agencies, and State and local governments, in accordance with law, policy, and security classification.

5.4. The Under Secretary of Defense (Comptroller)/Chief Financial Officer, in accordance with reference (e), shall ensure that Domains within the Business Mission Area promote Net-Centric data sharing and effectively enable COIs, including adjudicating conflicts in metadata agreements and identifying authoritative sources.

5.5. The Under Secretary of Defense For Intelligence shall:

5.5.1. Collaborate with the ASD(NII)/DoD CIO, the USD(P), and the IC CIO in developing policies and procedures to protect Net-Centric data while enabling data sharing across different security classifications, and between the Department of Defense, the IC, and multinational partners, in accordance with policies herein and consistent with Director of Central Intelligence Directive 8/1 (reference (f)).

5.5.2. In accordance with reference (e), ensure that Defense Intelligence Activities within the Domains of the National Intelligence Mission Area promote Net-Centric data sharing and effectively enable COIs, including adjudicating conflicts in metadata agreements and identifying authoritative sources.

5.5.3. Ensure counterintelligence and security support to network-centric operations.

Downloaded from http://www.everyspec.com

5.6. The Heads of the DoD Components shall:

5.6.1. Ensure implementation of Net-Centric data sharing, including establishing appropriate plans, programs, policies, processes, and procedures consistent with policies herein.

5.6.2. Ensure that all current and future data assets are made consistent with policies herein.

5.6.3. Support Mission Areas and Domains by taking an active role in COIs.

5.7. The Chairman of the Joint Chiefs of Staff shall:

5.7.1. In coordination with the ASD(NII)/DoD CIO, ensure the policies herein are incorporated into the Joint Capabilities Integration and Development System and the procedures of the IT and National Security Systems' (NSS) interoperability and supportability certification and test processes.

5.7.2. In coordination with the ASD(NII)/DoD CIO, direct the National Defense University to develop education and training programs to advocate Net-Centric data sharing in the Department of Defense based on policies herein.

5.7.3. Ensure that Domains within the Warfighter Mission Area promote Net-Centric data sharing and effectively enable COIs, including adjudicating conflicts in metadata agreements and identifying authoritative sources.

6. EFFECTIVE DATE

This Directive is effective immediately.

Paul Wolfowitz
Deputy Secretary of Defense

Enclosures — 1
E1. Definitions

Downloaded from http://www.everyspec.com

E1. ENCLOSURE 1

DEFINITIONS

E1.1.1. Accessible. A data asset is accessible when a human, system, or application may retrieve the data within the asset. Data assets may be made accessible by using shared storage space or web services that expose the business or mission process that generates data in readily consumable forms.

E1.1.2. Authoritative Source. A source of data or information that is recognized by members of a COI to be valid or trusted because it is considered to be highly reliable or accurate or is from an official publication or reference (e.g., the United States (U.S.) Postal Service is the official source of U.S. mailing ZIP codes).

E1.1.3. Community of Interest (COI). A collaborative group of users that must exchange information in pursuit of its shared goals, interests, missions, or business processes and therefore must have shared vocabulary for the information it exchanges.

E1.1.4. Data. A representation of facts, concepts, or instructions in a formalized manner suitable for communication, interpretation, or processing by humans or by automatic means. Data and information are equivalent terms for the purposes of this policy.

E1.1.5. Data Asset. Any entity that is comprised of data (see reference (b)). For example, a database is a data asset that is comprised of 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 web site 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.

E1.1.6. Domains. In this Directive, domains are subsets of Mission Areas and represent a common collection of related, or highly dependent, information capabilities and services. Managing these related information capabilities and services within domains improves coordination, collaboration, integration, and consistency of processes and interfaces for information sharing.

E1.1.7. Enterprise. Refers to the Department of Defense, its organizations, and related Agencies.

Downloaded from http://www.everyspec.com

E1.1.8. Enterprise Information Environment Mission Area. The Department of Defense's Mission Area responsible for managing the part of the DoD portfolio known as the enterprise information environment (EIE), which is the common, integrated computing and communications environment of the GIG. The EIE is composed of GIG assets that operate as, or that assure, local area networks, campus area networks, tactical networks, operational area networks, metropolitan area networks, and wide area networks. The EIE is also composed of GIG assets that operate as, or that assure, end user devices, workstations, and servers that provide local, organizational, regional, or global computing capabilities. The EIE includes all software associated with the operation of EIE assets and the development environments and user productivity tools used in the GIG. The EIE includes a common set of enterprise services, called Core Enterprise Services, which provide awareness of, access to, and delivery of information on the GIG.

E1.l.9. Global Information Grid (GIG). The globally connected, end-to-end set of information capabilities, associated processes, and personnel for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

E1.1.10. Information Capability. The ability to consume and generate information in the form of data assets by performing a specific task using IT and/or NSS.

E1.1.11. Information Technology (IT). Any equipment or interconnected system or subsystem of equipment that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the DoD Component. For purposes of the preceding sentence, equipment is used by a DoD Component if the equipment is used directly by the DoD Component or is used by a contractor under a contract with the DoD Component which requires the use of such equipment or requires the use, to a significant extent, of such equipment in the performance of a service or the furnishing of a product. The term "information technology" includes computers, ancillary equipment, software, firmware and similar procedures, services (including support services), and related sources. It also includes NSS as defined in paragraph E1.l.16., below. Notwithstanding the above, the term "information technology" does not include any equipment that is acquired by a Federal contractor incidental to a Federal contract.

E1.1.12. Law, Policy, or Security Classification. For this Directive, the pertinent statutory and regulatory authority dealing with data assets includes, but is not limited to: personal information, intelligence information, medical information, information on a non-DoD person, and classified information.

Downloaded from http://www.everyspec.com

E1.1.13. Metadata. Information describing the characteristics of data; data or information about data; or descriptive information about an entity's data, data activities, systems, and holdings. For example, discovery metadata is a type of metadata that allows data assets to be found using enterprise search capabilities.

E1.1.14. Metadata Registry. Repository of all metadata related to data structures, models, dictionaries, taxonomies, schema, and other engineering artifacts that are used to support interoperability and understanding through semantic and structural information about the data. A federated metadata registry is one in which multiple registries are joined electronically through a common interface and exchange structure, thereby effecting a common registry.

E1.1.15. Mission Area. A defined area of responsibility with functions and processes that contribute to mission accomplishment.

E1.1.16. National Security Systems (NSS). Any telecommunications or information system operated by the U.S. Government, the function, operation, or uses of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military and intelligence missions, but excluding any system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications).

E1.1.17. Net-Centric. Relating to or representing the attributes of net-centricity. Net-centricity is a robust, globally interconnected network environment (including infrastructure, systems, processes, and people) in which data is shared timely and seamlessly among users, applications, and platforms. Net-centricity enables substantially improved military situational awareness and significantly shortened decision making cycles. Net-Centric capabilities enable network-centric operations and NCW.

E1.1.18. Network-Centric Warfare (NCW). An information superiority-enabled concept of operations that generates increased combat power by networking sensors, decision makers, and shooters to achieve shared awareness, increased speed of command, higher tempo of operations, greater lethality, increased survivability, and a degree of self-synchronization. In essence, NCW translates information superiority into combat power by effectively linking knowledgeable entities in the battlespace.

E1.1.19. Semantic Metadata. Information about a data asset that describes or identifies characteristics about that asset that convey meaning or context (e.g., descriptions, vocabularies, taxonomies).

Downloaded from http://www.everyspec.com

E1.1.20. Shared Space. Storage on a file server or in electronic media that is addressable by multiple users or COIs. Also, web services that are made available to the enterprise that expose the business or mission processes that generate data in readily consumable forms.

E1.1.21. Structural Metadata. Information provided about a data asset that describes the internal structure or representation of a data asset (e.g., database field names, schemas, web service tags).

E1.1.22. Understandable. Capable of being comprehended in terms of subject, specific content, relationships, sources, methods, quality, spatial and temporal dimensions, and other factors.

E1.1.23. Users. Humans, systems, and applications that create, find, access, and exploit data. Also known as consumers and producers, or publishers and subscribers. System developers are also considered to be users. For this Directive, users may be expected and planned for, or unanticipated and not planned for.

E1.1.1.24. Visible. Able to be seen, detected, or distinguished and to some extent characterized by humans and/or IT systems, applications, or other processes.

E1.25. Web Services. A standardized way of integrating web-based applications using open standards over an Internet Protocol backbone. Web services allow applications developed in various programming languages and running on various platforms to exchange data without intimate knowledge of each application's underlying IT systems.