Department of Defense
INSTRUCTION

NUMBER 8320.02
August 5, 2013

DoD CIO

SUBJECT: Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense

References: See Enclosure 1

1. PURPOSE. This instruction:

a. Reissues DoD Directive (DoDD) 8320.02 (Reference (a)) as a DoD Instruction (DoDI) in accordance with the guidance in DoDI 5025.01 (Reference (b)) and the authority in DoDD 5144.02 (Reference (c)).

b. Establishes policies, assigns responsibilities, and prescribes procedures for securely sharing electronic data, information, and IT services and securely enabling the discovery of shared data throughout the DoD in accordance with DoDD 8000.01 (Reference (d)), Department of Defense Chief Information Officer (DoD CIO) Memorandum (Reference (e)), and DoD CIO Memorandum (Reference (f)).

c. Facilitates the shift from the transport medium to a focus on content and guides the use of resources to implement the secure sharing of data, information, and IT services within the DoD Information Enterprise (IE) and with mission partners.

2. APPLICABILITY

a. This instruction applies to:

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

(2) All data assets, information, and IT services that are or may be available within the DoD IE and all programs, projects, and initiatives developing or implementing them, including those managed as part of a community of interest (COI).

(3) Data, information, and IT services in electronic form.

(4) All new systems, services, or capabilities, as well as existing systems and services when investment dollars are received for modernization.

b. This instruction does not apply to data, information, and IT services supporting existing, deployed systems, except to the extent they receive investment dollars for modernization. In other words, this instruction does not require a mandatory retrofitting of existing systems, services, or capabilities.

c. Nothing in this instruction alters or supersedes the existing authorities and policies of the Director of National Intelligence regarding the protection of intelligence sources and methods, including the exchange of sensitive compartmented information and special access programs for intelligence as directed by Executive Order 12333 (Reference (g)).

d. In limited cases, exceptions to the policy and requirements in this instruction may be granted by the DoD CIO.

3. POLICY. It is DoD policy that:

a. Data, information, and IT services are considered enablers of information sharing to the DoD. Data, information, and IT services will be made visible, accessible, understandable, trusted, and interoperable throughout their lifecycles for all authorized users. Authorized users include DoD consumers and mission partners, subject to law, policy, data rights, and security classifications.

b. All DoD activities implement applicable standards and specifications as cited in the DoD IT Standards Registry (DISR) (accessible at https://gtg.csd.disa.mil), or any future DoD-designated registry for IT and data sharing standards.

c. Authoritative data sources (ADSs) are registered in the DoD Data Services Environment (DSE) (accessible at https://metadata.ces.mil/dse).

d. Resource impacts for implementing data, information, and IT services will be assessed and considered prior to issuing data sharing implementation direction and guidance.

e. Disabled DoD employees or members of the public seeking information or services from the Department of Defense must have access to and use of information and data comparable to the access and use by individuals who are not disabled, unless an undue burden would be imposed, to the extent required by section 794d of Title 29, United States Code (Reference (h)).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

6. RELEASABILITY. **Unlimited**. This instruction is approved for public release and is available on the Internet from the DoD Issuances Website at http://www.dtic.mil/whs/directives.

7. EFFECTIVE DATE. This instruction:

a. Is effective August 5, 2013.

b. Must be reissued, cancelled, or certified current within 5 years of its publication in accordance with Reference (b). If not, this instruction will expire effective August 5, 2023 and be removed from the DoD Issuances Website.

Teresa M. Takai
DoD Chief Information Officer

Enclosures
1. References
2. Responsibilities
3. Procedures
Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 8320.02, “Data Sharing in a Net-Centric Department of Defense,” December 2, 2004 (hereby cancelled)
(b) DoD Instruction 5025.01, “DoD Directives Program,” September 26, 2012
(c) DoD Directive 5144.02, “DoD Chief Information Officer (DoD CIO),” April 22, 2013
(d) DoD Directive 8000.01, “Management of the Department of Defense Information Enterprise,” February 10, 2009
(e) DoD Chief Information Officer Memorandum, “DoD Net-Centric Services Strategy,” May 4, 2007
(f) DoD Chief Information Officer Memorandum, “DoD Net-Centric Data Strategy,” May 9, 2003
(g) Executive Order 12333, “United States Intelligence Activities,” December 4, 1981, as amended
(h) Section 794d of Title 29, United States Code
(i) DoD Directive 5000.71 “Rapid Fulfillment of Combatant Commander Urgent Operational Needs,” August 24, 2012
(j) DoD Directive 5105.19, “Defense Information Systems Agency (DISA),” July 25, 2006
(k) DoD Instruction 5200.01, “DoD Information Security Program and Protection of Sensitive Compartmented Information,” October 9, 2008, as amended
(l) Intelligence Community Directive 501, “Discovery and Dissemination or Retrieval of Information within the Intelligence Community,” January 21, 2009
(m) Intelligence Community Directive 502, “Integrated Defense of the Intelligence Community Information Environment,” March 11, 2011
(n) Intelligence Community Directive 503, “Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,” September 15, 2008
(o) DoD Chief Information Officer Memorandum, “Department of Defense Information Enterprise Architecture,” Version 2.0, August 10, 2012[1]
(p) DoD 7000.14-R, Volume 1, Chapter 1, “Chief Financial Officer (CFO) of the Department of Defense,” current edition
(q) DoD Directive 1322.18, “Military Training,” January 13, 2009
(r) Executive Order 13587, “Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information,” October 7, 2011
(s) Chairman of the Joint Chiefs of Staff Instruction 3170.01H, “Joint Capabilities Integration and Development System,” January 10, 2012
(t) Chairman of the Joint Chiefs of Staff Instruction 6212.01F, “Net Ready Key Performance Parameter (NR KPP),” March 21, 2012
(u) DoD Directive 4630.05, “Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” May 5, 2004

[1] Available at http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx.

(v) DoD Instruction 4630.08, “Procedures for Interoperability and Supportability of Information Technology (IT) and National Security Systems (NSS),” June 30, 2004
(w) DoD Chief Information Officer Memorandum, “Interim Guidance for Interoperability of Information Technology (IT) and National Security Systems (NSS),” March 27, 2012
(x) Department of Defense Discovery Metadata Specification (DDMS),Version 4.1, June 12, 2012[2]
(y) DoD Directive 5015.2, “DoD Records Management Program,” March 6, 2000
(z) DoD 5015.02-STD, “Electronic Records Management Software Applications Design Criteria Standard,” April 25, 2007
(aa) DoD Directive 5400.11, “DoD Privacy Program,” May 8, 2007, as amended
(ab) DoD Directive 8500.01E, “Information Assurance (IA),” November 24, 2002
(ac) DoD Instruction 8500.02, “Information Assurance (IA) Implementation,” February 6, 2003
(ad) DoD Directive 8320.03, “Unique Identification (UID) Standards for a Net-Centric Department of Defense,” March 23, 2007
(ae) DoD Directive 8570.01, “Information Assurance (IA) Training, Certification, and Workforce Management,” August 15, 2004
(af) Committee on National Security Systems Instruction Number 4009, “National Information Assurance Glossary,” April 26, 2010
(ag) Executive Order 13526, “Classified National Security Information,” December 29, 2009
(ah) Administrative Instruction 15, “OSD Records Management Program,” May 3, 2013

[2] Available at http://metadata.ces.mil/dse/irs/DDMS/index.html

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CIO. The DoD CIO:

a. Guides and oversees matters related to the sharing of data, information, and IT services to ensure interoperability down to the technical level internally within DoD and externally with mission partners, including:

(1) Development, maintenance, and enforcement of policy for DoD metadata that uses Government and industry metadata standards.

(2) Development and maintenance, in coordination with the DoD Component heads and the Intelligence Community (IC) CIO, of policy and standards that enable the use of federated enterprise capabilities to:

(a) Publish metadata.

(b) Discover, search, and retrieve data and metadata, information, and IT services throughout the DoD IE.

(c) Guide DoD Components in realizing the delivery of the joint information environment (JIE).

(3) Development of policies and procedures to protect DoD data, information, and IT services, in accordance with law, policy, data rights, and security classifications, in coordination with the DoD Component heads and the IC CIO.

b. Establishes, maintains, and enforces governance of the DoD's IT policies and processes to enable secure sharing of DoD data, information, and IT services, including information assurance, discovery, accessibility, and dissemination (including releasability) requirements.

c. Adjudicates requests from the DoD Components for exceptions to compliance with this instruction and the use of enterprise services, interface standards, and specifications for the exchange of DoD data and information, and ensure responsibilities and procedures for the expeditious processing of waiver requests for time-critical needs (e.g., urgent operational need (UON)) and the policies established by DoDD 5000.71 (Reference (i)).

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO, the Director, DISA:

a. Performs enterprise technical feasibility assessments with recommendations for sharing all DoD data, information, and IT services, as directed by the DoD CIO.

b. Provides mechanisms to ensure DoD data, information, and IT services under DISA's cognizance are properly registered, exposed, and available in accordance with this instruction.

c. Integrates, through standards and specifications, DoD information systems, networks, and associated data serving the United States and authorized foreign partners, consistent with DoDD 5105.19 (Reference (j)).

d. Evolves, establishes, manages, and makes available the enterprise services and the interface standards and specifications for the sharing of data, information, and IT services in order to meet the needs of the DoD Components and their validated requirements.

e. Maintains the DSE, to include amplifying data (e.g., discovery, structural and semantic metadata assets), shared vocabularies, structural and descriptive metadata about IT services, enterprise ADS descriptive metadata, and related enterprise services.

f. In coordination with the DoD CIO, adjudicates DISR waivers and change requests submitted by DoD Components.

3. UNDER SECRETARY OF DEFENSE FOR ACQUISITION, TECHNOLOGY, AND LOGISTICS (USD(AT&L)). In coordination with the DoD CIO, the USD(AT&L):

a. Updates Defense Acquisition System policies and procedures, in accordance with this instruction.

b. Provides guidance to program managers and Program Executive Officers to evaluate and approve system or program implementation of data sharing practices.

c. Through the Defense Acquisition University, and in coordination with the Under Secretary of Defense for Policy (USD(P)), the CJCS, and the Secretaries of the Military Departments, provides updated education and training programs advocating the secure sharing of data, information, and IT services in the DoD in accordance with this instruction.

4. DEPUTY CHIEF MANAGEMENT OFFICER (DCMO). The DCMO, in coordination with the DoD CIO, monitors DoD business systems and promotes the secure sharing of DoD data, information, and IT services in accordance with this instruction.

5. USD(P). The USD(P) collaborates with the DoD CIO and the Under Secretary of Defense for Intelligence (USD(I)) to develop the policies and procedures to protect data, information, and IT services while enabling the secure sharing of them as strategic assets across different DoD security domains with the IC and mission partners, in accordance with law, policy, and security classifications.

6. USD(I). The USD(I):

a. Collaborates with the DoD CIO, USD(P), IC CIO, and DoD Component CIOs in developing policies and procedures to protect data, information, and IT services while enabling their secure sharing as strategic assets across DoD security domains with the IC and mission partners, in accordance with this instruction, DoDI 5200.01 (Reference (k)) and consistent with IC Directive (ICD) 501 (Reference (l)), ICD 502 (Reference (m)), and ICD 503 (Reference (n)).

b. In accordance with DoD CIO Memorandum (Reference (o)), oversees defense intelligence activities to promote the secure sharing of data, information, and IT services within their functional purview, in accordance with this instruction.

c. Oversees counterintelligence and security support required for the secure sharing of DoD data, information, and IT services.

d. Synchronizes the investment activities of the DoD Component heads that manage DoD intelligence data, information, and IT services that are funded from defense and national intelligence sources.

7. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER (USD(C)/CFO), DEPARTMENT OF DEFENSE. The USD(C)/CFO establishes provisions in DoD 7000.14-R (Reference (p)) that direct adherence to the data and services policy in this instruction, including a requirement for comptrollers to prohibit the execution of funds on programs, projects, and initiatives that do not comply with this instruction.

8. UNDER SECRETARY OF DEFENSE FOR PERSONNEL AND READINESS (USD(P&R)). The USD(P&R) coordinates with the USD(AT&L), CJCS, and the Secretaries of the Military Departments to develop education and training programs that advocate sharing data, information, and IT services in the DoD in accordance with DoDD 1322.18 (Reference (q)) and this instruction.

9. DoD COMPONENT HEADS. The DoD Component heads:

a. Ensure that all applicable initiatives, systems, services, or capabilities are consistent with this instruction and support secure sharing of these assets across DoD Components and mission partners.

b. Facilitate the interoperability of data assets by using DoD approved standards in acquisition and procurement and by participating in the IT standards development process by proactively submitting change requests via the DISR and requesting waivers from Director, DISA.

c. Ensure the identification of governance forums and processes that support functional owners’ and managers’ efforts to integrate metadata standards, processes, registries, COIs, and other DoD IE data initiatives across their organizations.

d. Fund engineering, implementation, and operation of capability demonstrations, projects, programs, initiatives, and other efforts that enable secure sharing of DoD data, information, and IT services.

e. Promote the secure sharing of DoD data, information, and IT services (including establishing appropriate plans, programs, policies, processes, and procedures), and within their functional purview, adjudicate conflicts to facilitate the secure sharing of these services where possible, or elevate them with recommendations to the appropriate governance forum.

f. Assess resource impacts for hosting or maintaining IT services prior to making them available within the DoD IE.

g. Ensure data, information, and IT services leverage approved enterprise identity and access management capabilities and community-accepted resource metadata tagging practices.

h. Register in the DSE, all identified ADSs, IT services, and required metadata.

i. Implement policies and procedures to protect data, information, and IT services while enabling their secure sharing as assets across the DoD security domains with the IC and mission partners in accordance with this instruction, References (k), (l), (m), (n), and Executive Order 13587 (Reference (r)).

j. Ensure responsibilities and procedures for the expeditious processing of waiver requests for time-critical needs (e.g., UON) and the policies established by Reference (i).

k. Coordinate with other DoD Components to identify potential enterprise data and service standards and specifications, including international, commercial, and federal, which support interoperability of DoD data, information, and IT services.

10. CJCS. In addition to the responsibilities in section 9 of this enclosure, and in coordination with the DoD CIO, the CJCS:

a. Coordinates with USD(AT&L), USD(P&R), and the Secretaries of the Military Departments to develop education and training programs that advocate sharing data, information, and IT services in accordance with this instruction.

b. Examines DoD warfighter systems in accordance with applicable guidance to verify the secure sharing of DoD data, information, and IT services in accordance with CJCS Instruction (CJCSI) 3170.01H (Reference (s)) and CJCSI 6212.01F (Reference (t)).

ENCLOSURE 3

PROCEDURES

1. DATA, INFORMATION, AND IT SERVICES SHARING

a. All information sharing enablers must comply or conform to applicable standards and specifications as registered in the DISR or receive a waiver in accordance with DoDD 4630.05 (Reference (u)), DoDI 4630.08 (Reference (v)), and DoD CIO Memorandum (Reference (w)).

b. Data, information, and IT services will be made visible to authorized users by creating and associating metadata, including discovery metadata, for each asset. DoD metadata standards must comply with applicable national and international consensus standards for metadata exchange whenever possible. Discovery metadata must conform to the DoD Discovery Metadata Specification (Reference (x)). All metadata will be discoverable, searchable, and retrievable (to the maximum extent allowed by law or DoD policy) using DoD-wide capabilities and tools, such as the DSE.

c. Data, information, and IT services will be accessible to authorized users by conforming to DoD-specified publication methods consistent with DoD guidance and policy, including but not limited to Reference (x), DoDD 5015.2 (Reference (y)), DoD 5015.02-STD (Reference (z)), and DoDD 5400.11 (Reference (aa)). DoD Components will consider resource impacts for hosting or maintaining IT services prior to making them available within the DoD IE.

d. Data, information, and IT services will be considered understandable when authorized users are able to consume them and when users can readily determine how those assets may be used for specific needs. Data standards and specifications that require associated semantic and structural metadata, including vocabularies, taxonomies, and ontologies, will be published in the DSE, or in a registry that is federated with the DSE. Descriptive metadata about IT services, as well as structural and semantic metadata to make published IT services understandable to IT service consumers, must be published in the DSE, or in a registry that is federated with the DSE.

e. Data, information, and IT services will be considered trusted when they have provided sufficient pedigree and descriptive metadata for consumers to rely on them as an ADS, and comply with applicable information assurance and cyber security policies, including DoDD 8500.01E (Reference (ab)) and DoDI 8500.2 (Reference (ac)).

f. DoD Components must ensure all DoD information programs, applications, and computer networks will protect data in transit and data at rest according to their confidentiality level, mission assurance category, and level of exposure in accordance with References (ab) and (ac).

2. DATA, INFORMATION, AND IT SERVICES INTEROPERABILITY. DoD Components will ensure data, information, and IT services interoperability by making data assets

understandable and enabling the reuse of business and mission processes in compliance with established technical, data, and services standards and in accordance with Reference (o).

3. DATA AND INFORMATION RECORDS MANAGEMENT. Data and information will be considered records and managed in accordance with policies outlined in Reference (y).

a. DoD Components shall incorporate records management and preservation considerations when designing, developing, enhancing and implementing electronic information systems that include structured data.

b. DoD Components shall manage unstructured data created from applications, electronic mail, and other messaging applications, word processing, or presentation software, with records management solutions compliant with Reference (z).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ADS	authoritative data source
COI	community of interest
CJCS	Chairman of the Joint Chiefs of Staff
CJCSI	Chairman of the Joint Chiefs of Staff instruction
DCMO	Deputy Chief Management Officer
DISA	Defense Information Systems Agency
DISR	DoD information technology standards registry
DoD CIO	Department of Defense Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DSE	Data Services Environment
IC	Intelligence Community
ICD	Intelligence Community Directive
IE	Information Enterprise
IT	information technology
JIE	joint information environment
UON	urgent operational need
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

PART II. DEFINITIONS

These terms and their definitions are for the purpose of this instruction.

accessible. Defined in Reference (o).

ADS. Defined in DoDD 8320.03 Reference (ad).

authorized user. Defined in DoDD 8570.01 (Reference (ae)).

COI. Defined in Committee on National Security Systems Instruction 4009 (Reference (af)).

data. Defined in Reference (af).

data asset. Defined in Reference (af).

discovery. Defined in Reference (o).

discovery metadata. Information about a data asset that describes the asset and allows it to be found using enterprise search capabilities.

DISR. A DoD registry consisting of citations of IT standards specified through a consensus process as the minimum set of IT standards for the acquisition of all DoD systems that produce, use, or exchange information. The objective is to obtain interoperability and supportability among DoD systems.

disseminate. To broadcast, publish, disperse, or otherwise take measures to ensure availability beyond the originating source or organization responsible for the information (e.g., to post, tweet, e-mail, share, or save in a location shared with external entities).

DoD IE. Defined in Reference (d).

DSE. A DoD registry that provides an on-line repository enabling developers to reuse, understand, and share existing data assets. It addresses structural and semantic metadata such as schemas, web service description language, stylesheets, and taxonomies; descriptive metadata about proposed and approved ADSs, including their relationships and their responsible governance authorities; and descriptive, semantic, and structural metadata about services and other functional capabilities, including service definitions and specifications that can be discovered for subsequent use. The DSE has a Web-based interface with streamlined metadata registration and discovery capabilities that support the visibility of DoD operational capabilities, data standards, and data needs. The DSE provides a number of service interfaces supporting both design-time and run-time access to metadata, and it interacts with other registries and repositories through Open Search federation.

enabler. Those tools, capabilities, or services that help to achieve an end goal. Data, information, and IT services are considered enablers of DoD information sharing.

exposure. The process of making data, information, or IT services visible, accessible, understandable, and trustable, which can be accomplished either directly by the original data producer or indirectly via a designated third party.

functional owners and managers. The principal DoD leaders with the assigned responsibility to make decisions about the functional policies of the DoD. They include the OSD Component heads and other designated capability or portfolio managers.

IC. Defined in section 6.1(z) of Executive Order 13526 (Reference (ag)).

information. Defined in Reference (d).

information assurance. Defined in Reference (ab).

interoperability. Defined in Reference (u).

IT. Defined in Reference (d).

IT services. An IT capability designed to provide awareness of, access to, and delivery of data or information made available for consumption by one or more users. Users can be an individual, organization, or machine.

JIE. A secure environment, composed of shared IT infrastructure, enterprise services, and a single security architecture, to achieve full-spectrum superiority, improve mission effectiveness, increase security, and realize IT efficiencies. The JIE is operated and managed per the Unified Command Plan, using enforceable standards, specifications, and common tactics, techniques, and procedures.

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. Metadata can be structural (specifying the format structure), semantic (specifying the meaning), or descriptive (providing amplifying or interpretive information) for data, information, or IT services.

mission partners. Defined in Reference (d).

OSD Components. Defined in Reference (b).

records. Defined in Reference (y).

secure sharing. The dissemination of information to intended recipients while proactively implementing management, policy, procedural, and technical controls to prevent access to the information by unauthorized persons.

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).

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).

structured data. Defined in Administrative Instruction 15 (Reference (ah)).

trusted. Defined in Reference (o).

understandable. Defined in Reference (o).

UON. Defined in Reference (s).

unstructured data. Defined in Reference (ah).

visible. Defined in Reference (o).