



Department of Defense **INSTRUCTION**

NUMBER 8320.07

August 3, 2015

DoD CIO

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

References: See Enclosure 1

1. PURPOSE. In accordance with the authority in DoD Instruction (DoDI) 8320.02 (Reference (a)) and DoD Directive (DoDD) 5144.02 (Reference (b)), this instruction:

a. Establishes policy, assigns responsibilities, and prescribes procedures to implement Reference (a) and to enable a secure sharing environment in the DoD that supports the warfighting, business, DoD intelligence, and enterprise information environment mission areas.

b. Describes or references key enablers necessary for sharing data, information, and IT services and ensuring data, information, and IT services are visible, accessible, understandable, trustworthy, and interoperable. Key enablers include, but are not limited to, concepts, processes, governance forums, standards, models, and shared vocabularies. For the purposes of the instruction, data sharing and information sharing are equivalent terms. Service and IT service, are used interchangeably throughout this instruction. IT services include DoD Enterprise Services; however, not all IT services are DoD Enterprise Services.

c. Guides the use of resources for implementing the sharing of data, information, and IT services within the DoD Information Enterprise (IE) and with mission partners.

d. Incorporates and cancels DoD 8320.02-G (Reference (c)).

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 new data assets, information, IT services, IT systems, and capabilities, as well as existing data assets, information, IT services, IT systems, and capabilities when investment funds are received for modernization, to include those managed as part of a community of interest (COI).

(a) DoD Chief Information Officer (CIO) Memorandum (Reference (d)), key principles, rules, constraints, and best practices apply within the Internet Protocol Boundary of the DoD Information Network (DoDIN), including those devices that are often disconnected if they are used to receive and share data.

(b) Outside of these boundaries, key principles still should be considered, but the rules of the DoD IE Architecture must yield to the state of technology and the needs and imperatives of DoD missions.

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

b. This instruction does not apply to data, information, and IT services supporting existing forward deployed systems, or those systems in use in combat operations, except to the extent that they receive investment dollars for modernization. Mandatory retrofitting of existing systems, services, or capabilities is not required.

c. This instruction will not alter or supersede:

(1) The existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of sensitive compartmented information (SCI) and special access programs (SAP) for intelligence pursuant to Executive Order 12333 (Reference (e)) and other applicable laws and regulations. The application of the provisions and procedures of this instruction to SCI or other SAP for intelligence information systems is encouraged where they may complement or discuss topics not otherwise specifically addressed.

(2) Existing laws and policies regarding the use of existing business information exchange standards to record the initiation of and responses to business events among the DoD, Federal, State, local government, foreign government, and commercial trading partners that comprise the DoD acquisition, logistics, and finance communities.

3. POLICY. It is DoD policy that:

a. The DoD will effectively improve information exchange across the DoD and with its mission partners to defend the United States and enhance global stability in accordance with DoDD 8000.01 (Reference (f)), the DoD CIO Memorandum (Reference (g)), and Executive Order 13526 (Reference (h)).

b. In accordance with DoD CIO Memorandum (Reference (i)), and except as required otherwise by law or DoD policy, the use of National Information Exchange Model (NIEM)-

based exchanges must be considered for all new Extensible Markup Language (XML) information exchanges created and for all XML information exchanges being modernized as part of the normal lifecycle management for these information exchanges.

c. All DoD activities will implement applicable standards and specifications as cited in the DoD IT Standards Registry (DISR) or successor registry, pursuant to DoDI 8330.01 (Reference (j)).

d. In accordance with Reference (a), authoritative data sources (ADSs) will be designated, registered, and used to the maximum extent possible to improve mission effectiveness by enabling the reuse of visible, accessible, understandable, trustworthy, and interoperable data. Criteria to designate and register an ADS is outlined in the DoD Data Services Environment (DSE) Concept of Operations (CONOPS) (Reference (k)) and DoD DSE User Manual (Reference (l)).

e. Data, information, and IT services will be visible to authorized users by creating and associating metadata (“tagging”), including discovery metadata, for each asset. In accordance with Reference (a), DoD metadata standards will comply with applicable national and international consensus standards for metadata exchange when possible.

f. Data, information, and IT services-sharing concepts and practices will be included in education and awareness training and the appropriate DoD processes.

g. Data, information, or IT services will comply with this instruction, DoDI 5000.02 (Reference (m)), and the Data and Services Deployment Principles and Business Rules as specified in Reference (d) during planning, approval, budgeting, funding, development, purchase, implementation, certification, or operation phases.

h. A common set of standards, protocols, and interfaces will be used to enable the sharing of DoD data, information, and IT services pursuant to Reference (d), Office of Management and Budget Memo M-13-13 (Reference (n)) and DoDI 8551.01 (Reference (o)). A common information-sharing technical framework will be used at all levels throughout the DoD in accordance with Reference (d). All new IT systems must be designed for openness, expose high-value data and content through implementation of neutral hosted services, and publish public data sets in the list at www.defense.gov/data. For existing systems, high-value data and content will be made available through Web application programming interfaces (APIs) and apply metadata tagging, as appropriate. To the greatest extent possible, the DoD’s common information sharing standards, protocols, and interfaces will be compatible and interoperable with those of other federal departments, agencies, and mission partners.

i. Data and information will be accessible via appropriate identity and access management (IdAM) mechanisms in accordance with DoD IdAM guidance.

j. Electronic data and information intended to be shared should, at a minimum, include associated security metadata identifying its classification determination, markings, disclosure, and handling rules in order to support access control.

k. Data and information that meets the definition of a federal record will be managed in accordance with records management policies outlined in DoDI 5015.02 (Reference (p)).

l. All DoD activities will comply with DoDD 5400.11 (Reference (q)) and DoD 5400.11-R (Reference (r)) with regard to personally identifiable information and sharing of information.

m. All DoD activities will comply with the Federal Acquisition Regulation (Reference (s)), Defense Federal Acquisition Regulation Supplement (Reference (t)), and DoDI 4140.01 (Reference (u)) for sharing of data and information regarding DoD procurement and supply chain management, respectively.


n. Individuals who are federal employees with disabilities or members of the public with disabilities seeking information or services from the DoD will have access to, and use of, information and data comparable to the access and use available to federal or public individuals without disabilities, subject to appropriate access considerations and in accordance with section 794d of Title 29, United States Code (Reference (v)). For exceptions to compliance with Reference (v), refer to DoD Manual (DoDM) 8400.01-M (Reference (w)).

4. RESPONSIBILITIES. See Enclosure 2.

5. PROCEDURES. See Enclosure 3.

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

7. EFFECTIVE DATE. This instruction is effective August 3, 2015.



Terry A. Halvorsen
DoD Chief Information Officer

Enclosures

1. References
2. Responsibilities
3. Procedures

Glossary

TABLE OF CONTENTS

ENCLOSURE 1: REFERENCES.....6

ENCLOSURE 2: RESPONSIBILITIES.....9

 DoD CIO..... 9

 DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA) 11

 USD(AT&L)..... 12

 DIRECTOR, OPERATIONAL TEST AND EVALUATION (DOT&E)..... 12

 DCMO..... 13

 USD(P)..... 13

 USD(I)..... 13

 DIRNSA/CHCSS..... 13

 USD(P&R)..... 14

 DoD COMPONENT HEADS..... 14

 SECRETARIES OF THE MILITARY DEPARTMENTS..... 15

 CJCS..... 16

 COMBATANT COMMANDERS..... 16

ENCLOSURE 3: PROCEDURES.....17

 OVERVIEW 17

 PROCEDURES..... 17

 DATA, INFORMATION AND IT SERVICES IMPLEMENTATION 19

 Make Data, Information, and IT Services Visible 19

 Make Data, Information, and IT Services Accessible 20

 Make Data, Information, and IT Services Understandable..... 21

 Make Data and Information Trustable and IT Services Secure..... 22

 Make Data, Information, and IT Services Interoperable 23

 Implement Data and Information Sharing Procedures..... 23

 Implement IT Services Procedures 23

 MANAGEMENT..... 24

 Governance Forums 24

 ADS Management..... 24

 IT Services Management 25

 Requests for Exemption..... 25

GLOSSARY26

PART I: ABBREVIATIONS AND ACRONYMS26

PART II: DEFINITIONS.....27

ENCLOSURE 1

REFERENCES

- (a) DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013
- (b) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
- (c) DoD 8320.02-G, "Guidance for Implementing Net-Centric Data Sharing," April 12, 2006 (hereby cancelled)
- (d) DoD Chief Information Officer Memorandum, "DoD Information Enterprise Architecture 2.0," August 10, 2012¹
- (e) Executive Order 12333, "United States Intelligence Activities," December 4, 1981, as amended
- (f) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009
- (g) DoD Chief Information Officer Memorandum, "DoD Information Sharing Strategy," May 4, 2007
- (h) Executive Order 13526, "Classified National Security Information," December 29, 2009
- (i) DoD Chief Information Officer Memorandum, "Adoption of the National Information Exchange Model in the Department of Defense," March 28, 2013
- (j) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014
- (k) Department of Defense Data Services Environment Concept of Operations (CONOPS), March 28, 2013²
- (l) Department of Defense Data Services Environment (DSE), Version 2.1, User Manual³
- (m) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015
- (n) Office of Management and Budget Memorandum M-13-13, "Digital Government: Building A 21st Century Platform To Better Serve The American People," May 23, 2012
- (o) DoD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)," May 28, 2004
- (p) DoD Instruction 5105.02, "DoD Records Management Program," February 24, 2015
- (q) DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014
- (r) DoD 5400.11-R, "Department of Defense Privacy Program," May 14, 2007
- (s) Federal Acquisition Regulation, current edition
- (t) Defense Federal Acquisition Regulation Supplement, current edition
- (u) DoD Instruction 4140.01, "DoD Supply Chain Materiel Management Policy," December 14, 2011
- (v) Title 29, United States Code

¹ Available at: <http://dodcio.defense.gov/Home/Initiatives/DIEA.aspx>

² Available at the DSE Web portal <https://metadata.ces.mil/dse-help/en/About%20DSE>

³ Available at the DSE Web portal <https://metadata.ces.mil/dse-help/en/About%20DSE>

- (w) DoD Manual 8400.01-M, “Procedures for Ensuring the Accessibility of Electronic and Information Technology (E&IT) Procured by DoD Organizations,” June 3, 2011
- (x) DoD Directive 8115.01, “Information Technology Portfolio Management,” October 10, 2005
- (y) DoD Chief Information Officer Memorandum, “DoD Net-Centric Data Strategy,” May 9, 2003
- (z) DoD Chief Information Officer Memorandum, “Department of Defense Net-Centric Services Strategy,” May 4, 2007
- (aa) DoD Directive 5000.01, “The Defense Acquisition System,” May 12, 2003, as amended
- (ab) DoD Instruction 8110.01, “Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD,” November 25, 2014
- (ac) DoD Manual 5200.01, Volume 1, “DoD Information Security Program: Overview, Classification, and Declassification,” February 24, 2012
- (ad) Department of Defense Discovery Metadata Specification (DDMS), Version 4.1, June 12, 2012
- (ae) Intelligence Community Directive 501, “Discovery and Dissemination or Retrieval of Information within the Intelligence Community,” January 21, 2009
- (af) Intelligence Community Directive 502, “Integrated Defense of the Intelligence Community Information Environment,” March 11, 2011
- (ag) Intelligence Community Directive 503, “Intelligence Community Information Technology Systems Security Risk Management, Certification and Accreditation,” September 15, 20082002
- (ah) Defense Acquisition Guidebook⁴
- (ai) DoD Directive 5111.1, “Under Secretary of Defense for Policy (USD(P)),” December 8, 1999
- (aj) National Disclosure Policy-1, “National Disclosure Policy and Procedures for the Disclosure of Classified Military Information to Foreign Governments and International Organizations,” October 2, 2000⁵
- (ak) DoD Directive 5100.20, “National Security Agency/Central Security Service (NSA/CSS),” January 26, 2010
- (al) Section 142, Title 10, United States Code
- (am) DoD Directive 7045.14, “The Planning, Programming, Budgeting, and Execution (PPBE) Process,” January 25, 2013
- (an) DoD Instruction 8500.01, “Cybersecurity,” March 14, 2014
- (ao) DoD Instruction 8510.01, “Risk Management Framework (RMF) for DoD Information Technology (IT),” March 12, 2014
- (ap) DoD Directive 5205.02E, “DoD Operations Security (OPSEC) Program,” June 20, 2012
- (aq) DoD Manual 5205.02-M, “DoD Operations Security (OPSEC) Program Manual,” November 3, 2008

⁴ Available at the Defense Acquisition University portal: <https://dag.dau.mil/>

⁵ Provided to designated disclosure authorities on a need-to-know basis from the Office of the Deputy Under Secretary of Defense for Policy Integration and Chief of Staff to the Under Secretary of Defense for Policy

- (ar) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012
- (as) DoD 5015.02 STD, "Electronic Records Management Software Applications Design Criteria Standard," April 25, 2007
- (at) Deputy Secretary of Defense Memorandum, "Department of Defense (DoD) Chief Information Officer (CIO) Executive Board Charter," February 12, 2012
- (au) DoD Directive 8320.03, "Unique Identification (UID) Standards for a Net-Centric Department of Defense," March 23, 2007
- (av) Committee on National Security Systems Instruction (CNSSI) No. 4009, "National Information Assurance Glossary," April 26, 2010
- (aw) Title 40, United States Code
- (ax) Department of Defense Chief Information Officer Strategy, "Cloud Computing Strategy," July 5, 2012

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CIO. The DoD CIO:

a. Establishes and oversees the DoD enterprise governance processes for the sharing of data, information, and IT services, to include the coordination and adjudication of issues across IT investment portfolios, authoritative bodies (ABs), mission areas, and COIs, in accordance with References (b), (d), DoDD 8115.01 (Reference (x)), and the DoD CIO Executive Board (EB) governance structure.

b. Establishes policy, assigns responsibilities, and provides direction for identifying, developing, and prescribing DoD standards for information technology (IT) systems that enable the use of enterprise capabilities to guide DoD Components in realizing the DoD IE end state described in Reference (f).

c. Develops and matures a DoD data framework that provides guidance regarding exchanges of data, their structure, and roles of information exchange models such as NIEM adoption across the DoD.

d. Coordinates the DoD representation to the NIEM Federal Governance Structure, including consolidating DoD requirements and position regarding the evolution of NIEM.

e. Develops metrics, in collaboration with the Deputy Chief Management Officer (DCMO), CJCS, and the Under Secretary of Defense for Intelligence (USD(I)), and select DoD Components for measuring progress in achieving the DoD goals for sharing data, information, and IT services. Metrics developed must meet testable technical requirements (i.e., visible, accessible, understandable, trusted or secure, and interoperable), in accordance with DoD CIO Memorandum (Reference (y)) and DoD Chief Information Memorandum (Reference (z)), and be published to the DoD Components.

f. Provides acquisition oversight for data, information, and IT services-sharing capabilities when designated as the Milestone Decision Authority by the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)) in accordance with Reference (m) and DoDD 5000.01 (Reference (aa)).

g. Coordinates with the CJCS in addressing information-sharing requirements of the Combatant Commands.

h. Adjudicates DoD Component requests for exceptions to compliance with this instruction and the use of enterprise services, interface specifications, and standards for the exchange of DoD data and information.

i. Directs, for unclassified information sharing capabilities, the development and distribution of a core set of standards for electronic information sharing, including associated applications. These are developed in coordination with the Under Secretary of Defense for Policy (USD(P)) and CJCS, in accordance with DoDI 8110.01 (Reference (ab)).

j. Issues a security classification guide regarding information sharing capability (e.g., software, hardware, architectures, configurations) in coordination with the USD(P), Director, National Security Agency/ Chief, Central Security Service (DIRNSA/CHCSS), and USD(I) and in accordance with Volume 1 of DoDM 5200.01 (Reference (ac)).

k. Evaluates candidate IT services submitted by the DoD Components for enterprise reuse and potential designation as an enterprise service.

l. Tracks and evaluates data, information, and IT services-sharing capabilities provided to the DoD Components.

m. Aids the USD(I), in coordination with the Intelligence Community (IC), to develop standardized guidance for use with other federal agencies with regard to data classification caveats, storage, handling, and distribution requirements and tagging, discovery, and access to data.

n. Guides and oversees matters relating to data sharing in support of the DoD Components, COIs, and IT portfolios, in accordance with Reference (a), by supporting, influencing, and enforcing enterprise metadata direction that uses existing government and industry metadata standards.

o. Develops the policies and procedures to protect data while enabling data sharing across security domains and with mission partners, other federal agencies, and State and local governments, in coordination with the USD(I), USD(P), DNI, DIRNSA/CHCSS, and CJCS, in accordance with applicable laws, DoD policy, and security classifications.

p. Develops and ensures that data, information, and IT services-sharing concepts and practices are incorporated into education and awareness training through the National Defense University, Defense Acquisition University, Military Service schools, and appropriate DoD processes in coordination with the CJCS, USD(AT&L), and USD(P&R).

q. Establishes and maintains the processes and governance to ensure compliance with the “Consider NIEM First” policy. Clarifies how NIEM relates to the use of the core set of standards and shared vocabularies for information exchange and applications developed, in accordance with Reference (d), DoD Discovery Metadata Specification (DDMS) (Reference (ad)), and DISR-approved standards and specifications.

r. Defines policy and oversight for a “tiered accountability” approach for compliance and enforcement of this instruction.

s. Provides governance oversight to those COIs aligned to the Enterprise Information Environment Mission Area.

t. Collaborates with the USD(P), USD(I), IC CIO, and DoD Component heads in developing policies, procedures, standards, and standards frameworks to protect data, information, and IT services while enabling their secure sharing as strategic assets, in accordance with this instruction, Reference (ac), and Intelligence Community Directive (ICD) 501 (Reference (ae)), ICD 502 (Reference (af)), and ICD 503 (Reference (ag)).

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in section 10 of this enclosure, the Director, DISA:

a. Plans, programs, and budgets for capabilities that share data, information, IT services, and the supporting infrastructures in coordination with the DoD CIO and the DoD Component heads.

b. Evolves, establishes, manages, and makes DoD enterprise services available to include the Global Information Grid Technical Guidance-Federation, the DSE registries, and any future DoD-designated registry for data and services standards and specifications that improve the sharing of data, information, and IT services. The standards should be in accordance with Reference (d).

c. Develops and publishes recommendations for the secure configuration, testing, and assessment of DoD IT systems supporting electronic sharing of data, information, and delivery of IT services capability.

d. When appropriate, enters into service-level agreements (SLAs) with the DoD Component heads for enterprise-level services that support their data, information, and IT services-sharing capability requirements.

e. Develops, coordinates, issues, and maintains technical procedures for the DoD Components to follow in managing and sharing data, information, and IT services.

f. Manages global cryptographic keying material and supporting virtual private network infrastructures for sharing data, information, and IT services in accordance with Reference (w).

g. Provides an electronic repository for data, information, and IT services-sharing agreements.

h. Maintains the DSE.

i. Develops recommendations for the use of enterprise capabilities that facilitate locating, searching, and retrieving data and metadata to include data at the tactical edge that exist in a denied, disconnected, intermittent, and limited bandwidth environment.

j. Reviews DISR waivers and change requests submitted by DoD Components. Forwards the DISR waivers and change requests to the DoD CIO with recommendations for further action, in accordance with the most current version of the Joint Enterprise Standards Committee's procedures.

3. USD(AT&L). In coordination with the DoD CIO, the USD(AT&L) ensures:

a. The Defense Acquisition System policies and procedures in the Defense Acquisition Guidebook (DAG) (Reference (ah)) are updated as warranted to incorporate the policies in this instruction for all Acquisition Category (ACAT), non-ACAT, and fielded IT and National Security Systems acquisitions and procurements. Ensures DAG updates include milestone exit criteria that require compliance with this instruction, and provides guidance for Milestone Decision Authorities on how to use tiered accountability, as described in current DoD IT interoperability policy, to evaluate and approve system or program satisfaction of data, information, and IT services-sharing practices.

b. The Defense Acquisition University develops or modifies education and training programs to advocate the sharing of data, information, and IT services in the DoD Service Schools, based on policies in this instruction.

c. Program managers, program executive officers, and functional owners and managers who support warfighting, business, and intelligence missions:

(1) Promote the sharing of data, information, and IT services and perform a cost analysis to evaluate the cost value of these requirements.

(2) Enable COIs.

(3) Support enterprise governance and the implementation of standards.

(4) Use and incorporate ADSs.

d. Developmental test policies, activities, and infrastructure are adequate to test and validate compliance with data sharing requirements and standards (including data tagging and IdAM standards). Ensures system Test and Evaluation Master Plans include associated developmental test strategy.

4. DIRECTOR, OPERATIONAL TEST AND EVALUATION (DOT&E). The DOT&E ensures processes, procedures, and infrastructure are available to operationally test and evaluate data-sharing capabilities and IT services for systems under operational test and evaluation oversight. In planning for and assessment of operational effectiveness, suitability, and survivability, DOT&E considers data, information, and IT services-sharing capabilities and their

impact on operational level parameters, such end-to-end mission performance, system interoperability, and cybersecurity.

5. DCMO. In coordination with the DoD CIO and the Military Departments' Chief Management Officers (CMOs), the DCMO:

a. Maintains and ensures that the DoD Business Enterprise Architecture and its appropriate plans, programs, policies, processes, product releases, and procedures are consistent with the intent of this instruction.

b. Provides governance oversight to those COIs aligned to the Business Mission Area.

6. USD(P). The USD(P):

a. Develops and issues DoD security plans, policies, and procedures necessary for effective implementation of foreign disclosure guidance in accordance with Reference (ac), DoDD 5111.1 (Reference (ai), National Disclosure Policy (NDP-01) (Reference (aj)), and Reference (ab).

b. Collaborates with the DoD CIO, USD(I), IC CIO, and DoD Component heads in developing policies, procedures, standards, and standards frameworks to protect data, information, and IT services while enabling their secure sharing as strategic assets, in accordance with this instruction and References (ac), (ae), (af), and (ag).

7. USD(I). The USD(I):

a. Oversees all DoD intelligence exchange and sharing agreements to enable the sharing of data, information, and IT services in accordance with policy in this instruction and all applicable references in Enclosure 1.

b. Collaborates with the DoD CIO, USD(P), IC CIO, and DoD Component heads in developing policies, procedures, standards, and standards frameworks to protect data, information, and IT services while enabling their secure sharing as strategic assets, in accordance with this instruction and References (ac), (ae), (af), and (ag).

c. Provides governance oversight to COIs aligned to the Defense Intelligence Mission Area.

8. DIRNSA/CHCSS. Under the authority, direction, and control of the USD(I), pursuant to DoDD 5100.20 (Reference (ak)), and consistent with section 142 of Title 10, United States Code (Reference (al)), and in addition to the responsibilities in section 10 of this enclosure, the DIRNSA/CHCSS develops and identifies cybersecurity solutions for secure and dynamic information-sharing communities and information confidentiality services for the connection of

networks that support data, information, and IT services between or within various network security and information domains.

9. USD(P&R). The USD(P&R), in conjunction with the National Defense University, develops education and training programs to advocate sharing data, information, and IT services in the DoD Service schools based on policies in this instruction.

10. DoD COMPONENT HEADS. The DoD Component heads, according to their responsibility and authority for assigned functional areas, including supporting information resources:

a. Promote data visibility, accessibility, understandability, trustworthiness, interoperability, data and services standards, and specifications compliance, in accordance with Enclosure 3 of this instruction, throughout planning, programming, and acquisition processes.

b. Direct and oversee development and visibility of data and services, shared vocabularies and associated metadata (e.g., discovery, structural, and semantic), and registration in appropriate registries, catalogs, and repositories in accordance with Enclosure 3.

c. 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.

d. Ensure capabilities are transitioned to the operational environment and are interoperable and compliant with data, information, and IT services-sharing standards and specifications.

e. Participate in the collaborative development of data engineering resources (DERs), and encourage their use within Component IT portfolios.

f. Appoint DSE namespace managers, who will provide governance oversight and who will clearly articulate procedures for configuration management within their assigned namespaces, as described in References (k) and (l).

g. Support the DoD CIO-designated enterprise governance processes for the sharing of data, information, and IT services.

h. Provide the Director, DISA, and the DoD CIO with DoD enterprise capabilities' project and planning information for the sharing of data, information, and IT services.

i. Comply with Director, DISA, policies to support organization-validated data, information, and IT services-sharing capability requirements with enterprise services. Develop and implement migration plans for the alignment of legacy information-sharing networks that previously have been granted waivers to compliance with current policies.

j. Plan, program, budget, and execute funding for capabilities that share data, information, IT services, and their supporting infrastructures to support data, information, and IT services-sharing capabilities. Provide program and budget data to the DoD CIO annually and when otherwise requested for DoD budget development, in accordance with DoDD 7045.14 (Reference (am)). Assess resource impacts for hosting or maintaining IT services before making them available within the DoD IE.

k. Manage data, information, and IT services-sharing communities in accordance with Enclosure 3 and References (d) and (p).

l. Provide candidate enterprise IT services capabilities through the DoD CIO EB governance structure to develop and extend data, information, and IT services-sharing capabilities.

m. In coordination with appropriate federal agencies, help the Office of the DoD CIO develop standards for agreements that address data, information, and IT services-sharing capabilities.

n. Collaborate with the USD(AT&L) to modify education and training programs to advocate the sharing of data, information, and IT services, based on this instruction.

o. Implement accredited information systems on networks that support data, information, and IT services-sharing capability, in accordance with DoDI 8500.01 (Reference (an)) and DoDI 8510.01 (Reference (ao)). Exceptions to the implementation of specifications and standards require DoD CIO approval.

p. Collaborate with the DoD CIO, USD(P), USD(I), and IC CIO in developing policies, procedures, standards, and standards frameworks to protect data, information, and IT services while enabling their secure sharing as strategic assets, in accordance with this instruction and References (ac), (ae), (af), and (ag).

q. Assess information sharing policies and procedures, and ensure risk of exposure to critical or classified information (alone or through compilation) is mitigated in accordance with Operations Security (OPSEC) process outlined in DoDD 5205.02E (Reference (ap)) and DoDM 5205.02-M (Reference (aq)). OPSEC assessments (using internal or external capabilities) are used for identifying and mitigating indicators of U.S. intentions, capabilities, operations, and activities.

11. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in section 10 of this enclosure, the Secretaries of the Military Departments, through their Departments' CMOs, ensure the Military Departments' business systems architecture and its appropriate plans, programs, policies, processes, and procedures are consistent with the intent of this instruction.

12. CJCS. In addition to the responsibilities in section 10 of this enclosure, the CJCS:

- a. Develops, coordinates, and issues policies, doctrine, and procedures for the sharing of data, information, and IT services capabilities in joint and combined operations.
- b. Helps the DoD CIO track and evaluate data, information, and IT services-sharing capabilities provided to the DoD Components.
- c. Uses data, information, and IT services-sharing capabilities during joint exercises and experimentation to promote joint force development, to include joint training, mission rehearsal, joint education, doctrine development, lessons learned, and experimentation and wargaming.
- d. Ensures that the Joint Staff and the Functional Capability Boards (FCBs) assess the data and service strategy tenets when reviewing and endorsing capabilities as they go through the FCB review and assessment process.
- e. Establishes tactics, techniques, and procedures that support data, information, and IT services-sharing to include community establishment, maintenance, termination, and development of SLAs and identity access or privilege management guidance, in coordination with the Combatant Commanders and the Director, DISA.
- f. Provides governance oversight to those COIs aligned to the Warfighting Mission Area.

13. COMBATANT COMMANDERS. In addition to the responsibilities in section 10 of this enclosure, the Combatant Commanders, through the CJCS:

- a. Integrate the operation and management of data, information, and IT services-sharing capabilities in support of regional combined operations as an integrated element of global data, information, and IT services-sharing capabilities.
- b. Act as the approval authority in their respective area of responsibility for the establishment, maintenance, and termination of data, information, and IT services-sharing communities or their leadership.

ENCLOSURE 3

PROCEDURES

1. OVERVIEW. This enclosure:

a. Provides DoD organizations, program managers, functional owners and managers, COIs, data producers, data providers, data consumers, and system developers specific procedures for the implementation of data, information, and IT services.

b. Includes key concepts and amplifying guidance to help enable the Joint Information Environment and achieve an information advantage for the DoD and its mission partners.

2. PROCEDURES

a. DoD Components, program managers, functional owners and managers, and COIs, within their functional purview, will:

(1) Ensure system developers, data producers, and data providers:

(a) Consider the NIEM standards-based approach first when developing XML information exchanges. In accordance with paragraph 3b above the signature of this instruction, the “Consider NIEM First” policy applies when DoD organizations are developing an XML information exchange for a new information exchange requirement or working an update to an existing information exchange. The “Consider NIEM First” rule applies to individual interfaces. Programs and systems follow the rule by using NIEM on each interface as applicable.

1. When considering NIEM for an information exchange, organizations will perform a business case assessment to compare the suitability of NIEM to that of any potential alternative approaches.

2. When NIEM is not the most efficient or effective means to address an information sharing requirement, organizations will document the technical, fiscal, and operational reasons why the alternative approach is better and will submit a request for an exception to the “Consider NIEM First” policy to the DoD CIO, as described in section 4 of this enclosure.

(b) Use existing commercial-off-the-shelf, government-off-the-shelf, open source software, and open standard solutions particularly those with widespread implementation, in accordance with Reference (m), when upgrading existing or designing new systems. Provide justification if not using these types of resources.

(c) To the greatest extent possible, use COI-specific semantic and structural DERs that have been collaboratively developed by data producers, data providers, data consumers, and system developers. Provide justification if not reusing these types of DER resources.

(d) Share data, information, and IT services with data consumers, in accordance with current DoD IdAM and federal identity, credential, and access management guidance or policies.

(2) Collaborate with data consumers to identify data, information, and IT services requirements.

(3) Provide oversight and articulate procedures for configuration management of any assigned namespaces in DSE, as specified in References (k) and (l).

(4) Help maintain and ensure proper functioning of data and metadata assets, shared vocabularies, services, and ADSs.

b. Data producers and data providers will:

(1) Make data and the associated metadata available at the closest operationally feasible point, which may include the posting of raw intelligence data before completion of data processing and analysis.

(2) Include relevant attributes that help ensure data accuracy such as error estimates and expiration and range of applicability of the data, to the extent applicable, in accordance with DoDI 8550.01 (Reference (ar)).

(3) Stage content or pre-position data within shared spaces where authorized data consumers are likely to find it through the normal course of operations.

c. Authoritative bodies (ABs), within their functional purview will:

(1) Publish proof of declaration as an AB by registering supporting artifacts (e.g., charter, mission statement, CONOPS) in the DSE.

(2) Adapt and execute processes for identifying, codifying, and registering data needs and ADSs into the DSE, to include recording the systems that meet those needs, in accordance with this instruction and References (k) and (l).

(3) Identify data sources and the context for when these data sources are authoritative.

(4) Ensure the proper registration of ADSs, to include the authoritative context and cross associations among related artifacts within the DSE, in accordance with DSE criteria as specified in References (k) and (l).

(5) Identify data conflicts, gaps, issues, or discrepancies within their functional purview, to include any policy, requirement, resource, or technical constraints on the data provider. Resolve those shortfalls where possible or elevate them within their IT governance structure.

d. COIs, within the scope of their functional purview, will:

(1) Identify data and information sharing capabilities, both operational and developmental, that should be in accordance with References (y) and (z).

(2) Identify standardized approaches to facilitate data and information sharing and to measure progress towards the data and services strategy goals as described in References (y) and (z).

(3) Measure the value of shared data, information, and IT services to consumers.

(4) Develop and maintain, in coordination with data producers, data providers, data consumers, and system developers, any semantic and structural DERs to ensure that data and metadata can be understood and used effectively by COI members and unanticipated authorized users.

(5) Register, in the DSE, any COI developed DERs and metadata products for use by the COI members and unanticipated authorized users.

(6) Ensure that COI-specific discovery metadata is designed in accordance with DISR mandated IT standards and specifications to maximize understandability and visibility during enterprise searches.

(7) Partner with a governing authority, as appropriate, to ensure that COI recommendations are adopted and implemented through programs, processes, systems, and organizations.

3. DATA, INFORMATION, AND IT SERVICES IMPLEMENTATION. Data, information, and IT services will be visible, accessible, understandable, and trustworthy and will ensure secure sharing. All DoD organizations, data producers, program managers, functional owners and managers, COIs, data producers, data providers, data consumers, and system developers will perform these procedures, as applicable:

a. Make Data, Information, and IT Services Visible

(1) Search the DSE for existing information resources registered by others, data schemas for carrying product payload, taxonomies, and other DERs as well as COIs working the same or similar problem space. Use the existing resources as a starting point for reaching agreement on common elements that are important for users to discover.

(2) Create discovery metadata for high-value data and information that describes who is responsible for specific data assets, where the data assets are located, what kind of data assets are available, and how to go about accessing the data assets to enable data for consumers to find.

(3) Associate discovery metadata (i.e., data tagging) with each respective data asset. When possible, integrate software automation of this task for each data asset in order to account for the various types and levels of detail.

(4) Publish in the DSE the discovery metadata about each data asset that will be available to all DoD authorized users.

(5) Post data assets to the DSE or other appropriate shared space. Users and applications will migrate from maintaining private data assets (i.e., data assets kept within system-specific storage) to making those data assets available in community and Enterprise-shared spaces (e.g., servers and IT services available on the Nonsecure Internet Protocol Router Network, “NIPRNET,” or Secret Internet Protocol Router Network, “SIPRNET.” Use these shared spaces as repositories for users and applications to post, or retrieve, data assets. Enterprise-shared spaces will be maintained, secured, and staged as necessary to support the DoD missions.

(6) Enable improved discovery of data assets posted to shared spaces by associating discovery metadata using enterprise search tools.

(7) Populate and maintain metadata registries. Metadata registries advertise the existence of shared data and metadata contained in the associated shared space.

(a) At a minimum, the DDMS mandatory elements will be represented within these metadata registries for all data assets posted to shared spaces. Each registry may be organized according to its community-defined practices. All metadata registries will adhere to Enterprise discovery interface standards to allow searches within a registry or across registries. Community registries will be linked to the DSE to create a “catalog of registries.”

(b) Registries will be searchable, either automatically by applications via APIs or manually through user-friendly, web-based interfaces.

(8) Establish archive spaces to support secure sharing of information, retrieval by multiple online applications and data services, and maintenance of the DoD Components records and information in accordance with applicable instructions. Enterprise archive spaces will be developed, maintained, secured, and staged as necessary to support this requirement.

(9) Archive data and metadata in standard formats to long-term accessible spaces in accordance with Reference (p) and DoD 5015.02 STD (Reference (as)). Users, applications, and data repositories will migrate from operational to inactive status yet will present requirements for shared information access (i.e., data and metadata no longer used may be indexed by search systems or to answer Freedom of Information Act inquiries and other queries).

b. Make Data, Information, and IT Services Accessible

(1) Document access procedures, processes, and sharing constraints to include identifying any existing policies, laws, or classifications that would restrict access to the data and metadata across the enterprise. This includes traditional access mechanisms that often have many implicit rules indicating how systems respond to requests.

(2) Associate security-related metadata with each respective data asset. Access to data assets will be controlled by classification marking metadata and technologies such as public key infrastructure and role and attribute-based access control (ABAC) processes.

(3) Engineer access mechanisms for maximum scalability to handle unanticipated, authorized users without degrading performance for critical operational users.

(4) Discover enterprise resources by leveraging available work products, operational access mechanisms, and data standards and information exchange specifications (IES).

(a) Collaborate with all relevant stakeholders to promote reuse of access mechanisms, and reduce the work required to obtain desired capabilities.

(b) Adhere to existing technical standards, specifications and profiles, as specified in the DISR and the DSE.

(5) Reduce the need for predefined, engineered point-to-point interfaces by using standardized web-based, machine-readable, open format approaches that maximize reuse wherever operationally and technically feasible.

(6) Implement new interfaces that can handle authorized but unanticipated users by transitioning tightly-coupled (i.e., point-to-point interfaces) to loosely-coupled services (i.e., many-to-many data exchanges).

c. Make Data, Information, and IT Services Understandable

(1) Consider first the NIEM standards-based approach when deciding which information sharing exchange approach best meets the mission and operational needs for secure sharing.

(2) If NIEM is not the most effective and efficient approach, then:

(a) Discover and reuse existing semantic metadata products to include vocabularies, taxonomies, ontologies, and conceptual data schemas found in the DSE as the basis for any new or related semantic metadata.

(b) Discover and reuse existing structural metadata products to include logical and physical data schemas found in the DSE as the basis to form any new or related structural representations.

(3) Develop a shared understanding of the data and metadata to be made visible and accessible. This may be accomplished by defining community-based ontologies, taxonomies (i.e., data categorization schemes), thesauruses, vocabularies, or key word lists.

(4) Register all applicable DERs in the DSE.

(5) Associate semantic metadata with each respective asset. Semantic metadata provides insight into the meaning and context of an asset to include content-related details such as DDMS elements: topic, keywords, and context.

(6) Associate structural metadata with each respective asset. Structural metadata describes the format-related aspects of the asset such as file size, bit rate, and dimensions allowing consumers to narrow down information searches in order to select products that meet their particular operating constraints.

(7) Publish any new or modified semantic, structural, or community specific content-related metadata products into the DSE.

d. Make Data and Information Trustable and IT Services Secure

(1) Identify ADSs and in what context the data is authoritative.

(2) Register ADSs in the DSE and show the business uses and context for which the authority is valid.

(3) Include security level markings on all exchanged data in XML format (i.e., “data-in-transit”). These markings will be specified in accordance with the IC information security marking metadata standard and Reference (al) and will include all pertinent classification data, such as declassification date.

(4) Associate security-related metadata to each respective asset to support consumers’ decisions on which data assets are appropriate for use to include:

(a) Pedigree metadata. Enables consumers to track the source and lineage of an asset. Notional metadata describing an asset’s pedigree consists of creation date, modification date, processing steps (including methods and tools), source and author (if known) status, and validation results against a published set of constraints.

(b) Security labels. Restrict access to data and metadata on the basis of classification and dissemination controls.

(c) Rights protection metadata. Includes any copyright, trademark, licensing, proprietary information, privacy act (in accordance with References (q) and (r)), or other usage restriction used to protect data against inappropriate use.

(5) Deploy data, information, and IT services in accordance with the most current security requirements and guidance provided by the Federal Risk and Authorization Management Program.

e. Make Data, Information, and IT Services Interoperable

(1) Data consumers must consider the parameters as specified in the DoD Enterprise registries for a given IT service in order to consume its data.

(2) Developers must include applicable architectural views, in accordance with Reference (d), and a summary list of all information exchanges within the Information Support Plan in accordance with Reference (j).

(3) Data consumers and developers, when appropriate, must use data mediation to expand the ability to leverage content that must be aggregated from multiple sources, developed via an orchestrated set of processes, transformed in information structure, or adapted from one protocol to another.

(4) Functional owners and managers of an IT service can petition the DoD CIO to consider designating the IT service as a DoD enterprise service if the IT service is determined to be useful beyond its intended functional boundaries.

(5) Developers and system sponsors must ensure that data interoperability is evaluated as part of all applicable system test and evaluation plans.

f. Implement Data and Information Sharing Procedures. In addition to the procedures in paragraphs 2a through 2e of this enclosure, these procedures apply to data and information:

(1) Data will be made available as soon as possible. Data producers and data providers should not delay making the asset accessible in order to complete processing of data before posting it, except when limited by security, policy, regulations, or to maintain minimum levels of data accuracy.

(2) When developing information exchanges, reuse IES and information exchange packages as available in the DSE while conforming to overall guidance for NIEM adoption across the DoD. The creation of new information exchanges or modernization of existing information exchanges will follow requirements to provide for use of DDMS and ABAC.

g. Implement IT Services Procedures. In addition to the procedures in paragraphs 2a through 2e of this enclosure, these procedures apply to IT services:

(1) Functional owners and managers of IT services will expose services to consumers through the use of non-proprietary World Wide Web Consortium and Organization for the Advancement of Structured Information Standards web standards (e.g., Simple Object Access Protocol, Web Service Description Language (WSDL), Representational State Transfer, Javascript Object Notation (JSON)).

(2) Functional owners and managers of IT services must provide service description information to enable discovery and understanding by consumers throughout the enterprise.

(3) Functional owners and managers of IT services must define and register, in the DSE, the vocabulary and business rules that underlie the implementation of the IT service in order to ease understanding of the inputs, outputs, and operations of the service by the related functional community.

4. MANAGEMENT

a. Governance Forums. The DoD CIO, through the DoD CIO EB established, pursuant to Deputy Secretary of Defense Memorandum (Reference(at)), will ensure processes and procedures work with Planning, Programming, Budgeting, and Execution; acquisition; and IT portfolio management.

(1) Governance should address executive level, program management, and engineering responsibilities, as well as address data, architecture, services, and standards used across the IE mission areas.

(2) The DoD CIO, through the DoD CIO EB governance structure established, pursuant to Reference (at)), will adjudicate cross-boundary technical conflicts as well as provide oversight of those COIs recognized by the DoD CIO to ensure resolution of operational data sharing gaps within mission threads and use cases.

b. ADS Management. Reliable, accessible ADSs are critical to enabling informed decisions based on trustworthy data and information. A key step in ADS management includes the definition, identification, maintenance, and validation of ADSs, and specific data needs collected from data producers, data providers, and data consumers.

(1) Management of ADSs is accomplished through the act of binding together data needs, data sources, and data, and decisions of suitability for adoption or usage within a specific context by one or more ABs within the DSE.

(2) The DSE supports the binding of data needs, data sources, and data by allowing operational users to propose ADSs. These proposed ADSs are then brought to the attention of all ABs that have specified the data need as within their area of responsibility.

(3) The members of the ABs or their designees may then approve the proposal, thus formally designating an ADS. This process provides shared visibility on decisions made by ABs on data and data sources, which helps accuracy and fosters user confidence regarding a particular data source. Additionally, the DoD CIO EB and its supporting forums will act to resolve issues between ABs regarding the creation, modification, or retirement of ADSs.

c. IT Services Management. Management of IT services requires an orderly process to confirm that services satisfy the policy tenets (e.g., making services visible, accessible, understandable, secure, and interoperable) and that policy decision and enforcement are consistent with the requirements of the DoD as well as relevant COIs and stakeholders. Part of the management process is ongoing oversight of performance measures that confirm compliance with service level commitments. Where corrective action is required, the management process will track issues and defects to insure that they are resolved in a manner and timeframe consistent with service level commitments.

d. Requests for Exemption. In those limited cases where a data asset, IT service, program, or system may be eligible for exemption from this instruction, the AB or sponsoring component organization should forward their request for exemption, via appropriate component organizations, to the DoD CIO. Before final decision on any request or waiver, the DoD CIO may task a DoD CIO EB committee to review and provide their recommendation for approval or disapproval. Requests for DoD CIO waivers and exceptions to policy must, at a minimum, include:

(1) A DoD Component-level endorsement, and full description of the reasons for the waiver or request for exception. The waiver or request for exemption includes the operational requirement for the information exchange as well as negative cost, schedule, performance, and information security impacts of complying with this instruction.

(2) Any operational or financial limitations or impacts that will occur if the waiver is not granted.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

AB	authoritative body
ABAC	attribute based access control
ACAT	acquisition category
ADS	authoritative data source
API	application programming interface
CIO	Chief Information Officer
CJCS	Chairman of the Joint Chiefs of Staff
CMO	Chief Management Officer
COI	community of interest
CONOPS	concept of operations
DAG	Defense Acquisition Guidebook
DCMO	Deputy Chief Management Officer
DDMS	DoD Discovery Metadata Specification
DER	data engineering resource
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DISA	Defense Information Systems Agency
DISR	DoD Information Technology Standards Registry
DNI	Director of National Intelligence
DoDD	DoD Directive
DoDI	DoD Instruction
DoDIN	DoD Information Network
DoDM	DoD Manual
DOT&E	Director, Operational Test and Evaluation
DSE	Data Services Environment
EB	executive board
FCB	Functional Capability Board
IC	Intelligence Community
ICD	Intelligence Community Directive
IdAM	identity and access management
IE	information enterprise
IES	information exchange specification
IT	information technology
JSON	Javascript Object Notation
NIEM	National Information Exchange Model

OPSEC	operations security
SAP	special access program
SCI	sensitive compartmented information
SLA	service-level agreement
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
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
WSDL	web service description language
XML	extensible markup language

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purpose of this instruction.

AB. An officially recognized group of stakeholders empowered by a DoD-approved mission statement to develop and approve ADSs within the context of a data or mission area. An AB is a recognized, sustainable organization with funding and staff possessing technical or subject matter expertise, a transparent decision-making process, a well-defined, rigorous configuration management process, and active participation in sanctioned DoD Enterprise-level coordination forums. Officially established COIs (such as chemical, biological, radiological, and nuclear) are the AB for identifying ADSs within their area of interest. Official recognition means there is a General Officer/Flag Officer/Senior Executive Service approved chartering document.

accessible. Defined in Reference (d).

ADS. Defined in DoDD 8320.03 (Reference (au)).

COI. Defined in Committee on National Security Systems Instruction No. 4009 (Reference (av)).

cybersecurity. Defined in Reference (an).

data. Defined in Reference (au).

data asset. Defined in Reference (au).

data consumer. An individual, group, or application utilizing data for specific purposes.

data interoperability. The ability to correctly interpret data that crosses system or organizational boundaries.

data mediation. A translation (e.g., data aggregation, orchestration, transformation, adaptation) of content from one form to another. Data mediation expands the ability to leverage content that must be aggregated from multiple sources, developed via an orchestrated set of processes, transformed in information structure, or adapted from one protocol to another. Due to the scale and scope of DoD operations and concerns, data mediation has played and will continue to play a vital role in data interoperability.

data need. A named and defined specification for a particular type of data that supports one or more operational requirements. It may be generic or very specific. A single data source may be made up of other systems, services, databases, data feeds, or capabilities.

data producer. A program, organization, or even a person who controls, manufactures, or maintains data assets within the DoD.

data provider. An entity or organization that exposes data assets to consumers from a data source or producer. A data provider may expose data; however, it may or may not also be the original data producer.

data source. A specific data set or repository from which data can be attained for subsequent use by consumers. A data source may be the combination of multiple, separate data sets or repositories.

data standard. A documented agreement and specification by an AB on a definition, representation, or format of data, metadata, or exchange protocol that is used to improve data understanding and data interoperability. A data standard requires a narrative specification and may include complementary DERs to guide IT system development and testing conformance. Widespread adoption of a well-designed data standard can reduce ambiguity and the necessity for mediation, while promoting efficiency and transparency of mediation where required.

DER. A specification that is expressed in a formal syntax that is registered in the DSE. A data engineering resource may convey the data structure and validation constraints for an information exchange, has the program logic to translate between different representations, has the controlled vocabulary whose terms will be used in data exchanges or metacards, or describes the inputs, outputs, and operations for a web service, or an information system. A controlled vocabulary is a list of terms that have been enumerated explicitly, controlled by a registration authority, in which every term has an unambiguous, non-redundant definition. These predefined, authorized terms and definitions can be used to describe information resources and reduce the ambiguity inherent in natural language. The terms may be organized as a list, a hierarchy, or a graph to document a set of definitions, a set of subject headings, and more complex organizations like a thesaurus. Term(s) may be used to categorize information resources to aid discovery and guide browsing. Examples of DERs are XML schemas, schematron documents, stylesheets, WSDL documents, taxonomies, ontologies, and conformant samples.

discovery. Defined in Reference (d).

discovery metadata. Defined in Reference (a).

DISR. Defined in Reference (a).

DoD Enterprise Service. IT Services that are offered to all DoD Components and have an approval to operate on a DoD network.

DoD IE. Defined in Reference (f).

DoDIN. The globally interconnected, end-to-end set of information capabilities, and associated processes for collecting, processing, storing, disseminating, and managing information on-demand to warfighters, policy makers, and support personnel, including owned and leased communications and computing systems and services, software (including applications), data, and security.

DSE. Defined in Reference (a).

enterprise services. Defined in Reference (f).

functional owners or managers. Defined in Reference (a).

high-value information. Defined in Reference (n).

IC. Defined in Reference (h).

IES. A narrative specification and collection of DERs that define and describe the structure and content of a data exchange to share information between two or more parties. Software developers use the content in the IES to implement software that correctly produces or consumes the instance documents in the specified type of data exchange.

information. Defined in Reference (au).

interoperability. Defined in Reference (j).

IT. Defined in section 11103 of Title 40, United States Code (Reference (aw)).

IT services. Engagement of the time and effort of a service provider, through the use of IT, whose primary purpose is to perform an identifiable task, or tasks, rather than furnish an end item of supply.

Joint Information Environment. A secure joint information environment comprised 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.

JSON. An open, text-based data exchange format. Like XML, it is human-readable, platform independent, and offers a wide availability of implementations. Data formatted according to the

JSON standard is lightweight and can be parsed by JavaScript implementations with incredible ease, making it an ideal data exchange format for virtually any scenario where applications need to exchange or store structured information as text.

metadata. Defined in Reference (a).

mission partners. Defined in Reference (f).

narrative specification. Material that describes the purpose and intended use of a specification. A narrative specification should: provide a functional description of the features and functions of the specification that would be understandable to someone not already familiar with the specification, note any boundary conditions in which use of the specification would be unsuitable (e.g., not suitable for targeting), provide point of contact information, including URLs to additional information, and show handling restrictions clearly, including, but not limited to copyright and licensing of the specification and any associated DERs.

profile. A set of one or more standards and, where applicable, the set of chosen classes, subsets, options, and parameters of those standards necessary to accomplish a particular function.

records. Defined in Reference (p).

secure sharing. Defined in Reference (a).

semantic metadata. Defined in Reference (a).

service. Engagement of the time and effort of a service provider whose primary purpose is to perform an identifiable task, rather than provide an end item of supply.

service provider. Defined in Department of Defense Chief Information Officer Cloud Computing Strategy (Reference (ax)).

shared space. Defined in Reference (z).

specification. An explicit set of requirements to be satisfied by a material, design, product, or service.

structural metadata. Defined in Reference (a). Structural metadata provides details pertaining to the format of the associated asset and is useful when trying to understand the physical manifestation of an asset.

tiered accountability. A federated management approach to achieve an effective and efficient outcome, where multiple levels of organizations exist, each having respective authorities. The DoD can be defined as a set of tiers which, as a minimum, include enterprise, capability, and component levels. Each tier of the DoD governs the areas for which it is responsible and maintains consistency with guidance from higher tiers.

trusted. Defined in Reference (d).

understandable. Defined in Reference (d).

visible. Defined in Reference (d).