Department of Defense
DIRECTIVE

NUMBER 8000.01
March 17, 2016
Incorporating Change 1, July 27, 2017

DoD CIO

SUBJECT: Management of the Department of Defense Information Enterprise (DoD IE)

References: See Enclosure 1

1. PURPOSE. This directive:

a. Reissues DoD Directive (DoDD) 8000.01 (Reference (a)) to establish policy and assign responsibilities for DoD information resources management (IRM) activities to the Chief Information Officer of the Department of Defense (DoD CIO).

b. Implements sections 2222, 2223, and 2224 of Title 10, United States Code (U.S.C.) (Reference (b)), chapter 113 of Title 40, U.S.C. (Reference (c)), chapters 35 and 36 of Title 44, U.S.C. (Reference (d)), and Office of Management and Budget Circular A-130 (Reference (e)) by establishing policy for the management of the DoD IE.

c. Provides direction on creating an information advantage for DoD personnel and mission partners and establishing and defining roles for chief information officers (CIOs) and IRM officials at various levels within DoD, in accordance with References (b), (c), (d), and (e).

d. Provides direction for information sharing among all DoD Components and with mission partners, in accordance with the DoD Instruction (DoDI) 8320.02 (Reference (f)) and the National Strategy for Information Sharing and Safeguarding, (Reference (g)).

2. APPLICABILITY. This directive applies to*:*

a. 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 DoD (referred to collectively in this directive as the "DoD Components").

b. The United States Coast Guard. The United States Coast Guard will adhere to DoD cybersecurity requirements, standards, and policies in this issuance in accordance with the

direction in Paragraphs 4a, b, c, and d of the Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security (Reference (x)).

3. POLICY. It is DoD policy that:

a. Information is considered a strategic asset to DoD. It must be safeguarded, appropriately secured and shared, and made available to authorized DoD personnel and mission partners to the maximum extent allowed by law, DoD policy, and mission requirements, throughout the information life cycle.

b. Functional processes are to be examined, and if possible streamlined or improved, in order to improve effectiveness and reduce cost before investment is made in information technology.

c. Each DoD Component has a CIO or senior IRM official who coordinates directly with the Component head and with the DoD CIO on behalf of the Component head. CIOs also may be designated at subordinate levels, although a reporting mechanism through the Component CIO must be maintained to ensure unity of purpose.

d. All aspects of the DoD IE, including the DoD information network infrastructure, DoD enterprise IT service and solutions, National Security Systems, Industrial Control Systems, and embedded computing of wired, wireless, mobile communication, and platforms will be planned, designed, developed, architected, configured, acquired, managed, operated, and protected in order to help achieve an information advantage and full spectrum superiority, deliver mission assurance, improve mission effectiveness, and realize IT efficiencies.

e. The architecture that describes the DoD IE, as defined in this directive, will be designated the DoD Information Enterprise Architecture (DoD IEA). The DoD IEA will:

(1) Be developed, maintained, and applied to guide IT investment portfolio strategies and decisions, define IT capability and interoperability requirements, establish and enforce IT standards, and guide cybersecurity requirements in accordance with DoDI 8500.01 (Reference (h)), across the DoD.

(2) Serve as the DoD CIO's contribution to the DoD Enterprise Architecture (DoD EA), which consists of architectures from Intelligence, Warfighting, and Business Mission Areas as well as DoD Component architectures.

f. In accordance with DoDI 8115.02 (Reference (i)), IT investments should link mission needs, information, and technology while efficiently managing resources and implementing DoDI 8510.01 (Reference (j)).

g. Investments in information solutions should be managed through a capital planning and investment control process that:

(1) Is performance- and results-based.

(2) Provides for analyzing, selecting, controlling, and evaluating investments, as well as assessing and managing associated risks.

(3) Interfaces with the DoD key decision support systems for capability identification; planning, programming, budgeting, and execution; and acquisition.

(4) Requires the review of all information technology (IT) investments for compliance with architectures, IT standards, and related policy requirements.

(5) Addresses life-cycle management

h. IT will be developed in useful increments that are as narrow in scope and brief in duration as practical; each increment will solve a specific part of an overall mission problem and deliver a measurable net benefit independent of future increments.

i. Pilots, modeling and simulation, experimentation, and prototype/proof of concept projects should be considered, especially when large, high-risk investments in IT are involved. These pilots, models, and other prototype or proof of concepts projects must be appropriately sized, and of limited duration to achieve desired objectives, and not used in lieu of testing or acquisition processes to implement the production version of the information solution.

j. A highly qualified and capable cyberspace workforce must be recruited, developed, and retained to evolve the DoD IE in order to maintain an information advantage consistent with DoDD 8140.01 Reference (k)). The entire DoD workforce will need to be trained and prepared to work in the evolving DoD IE.

k. In accordance with section 794d of Title 29, U.S.C. (Reference (l)), DoD employees or members of the public with disabilities seeking information or services from the DoD must have access to and use of information and data comparable to the access and use by individuals without disabilities, unless such access and use would impose an undue burden on the DoD.

(1) In addition, section 794d of Reference (l) requires that federally conducted or assisted activities be reasonably modified to accommodate covered individuals with disabilities when the modifications are necessary to avoid unlawful discrimination of the basis of disability, unless making the modifications would result in an undue burden or fundamentally alter the nature of the activity, and section 791 of Reference (l) requires that a covered employee or applicant for employment with a disability be reasonably accommodated.

(2) These obligations may include reasonable modifications or accommodations to facilitate access to IT systems by covered individuals with disabilities.

l. To operationalize the DoD IE, DoD will, to the maximum extent practical, architect its systems for interoperability and openness, and deliver secure, device-agnostic, digital services for the best value in accordance with Office of Management and Budget Memorandum M-13-13 (Reference (m)), DoDI 8330.01 (Reference (n)), and DoDI 8310.01 (Reference (o)).

m. New and existing IT investments and services will support achieving the goals and objectives of the DoD IRM Strategic Plan (Reference (p)) and support the implementation of the joint information environment (JIE) strategy (Reference (q)), and DoDI 8110.01 (Reference (r)).

4. RESPONSIBILITIES. See Enclosure 2.

5. RELEASABILITY. **Cleared for public release**. This directive is available on the ~~DoD Issuances Website at http://www.dtic.mil/whs/directives~~ *Directives Division Website at http://www.esd.whs.mil/DD/*.

6. EFFECTIVE DATE. This directive is effective March 17, 2016.

Robert O. Work
Deputy Secretary of Defense

Enclosures
1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise," February 10, 2009 (hereby cancelled)
(b) Title 10, United States Code
(c) Title 40, United States Code
(d) Title 44, United States Code
(e) Office of Management and Budget Circular No. A-130, "Management of Federal Information Resources," November 28, 2000
(f) DoD Instruction 8320.02, "Sharing Data, Information, and Technology (IT) services in the Department of Defense," August 5, 2013
(g) White House Office of the Press Secretary, "National Strategy for Information Sharing and Safeguarding," December 19, 2012
(h) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
(i) DoD Instruction 8115.02, "Information Technology Portfolio Management Implementation," October 30, 2006
(j) DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014*, as amended*
(k) DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015
(l) Title 29, United States Code
(m) Office of Management and Budget Memorandum M-13-13, "Open Data Policy—Managing Information as an Asset," May 9, 2013
(n) DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014
(o) DoD Instruction 8310.01, 'Information Technology Standards in the DoD," February 2, 2015
(p) DoD FY2014 Information Resources Management Strategic Plan, May 30, 2014
(q) The DoD Strategy for Implementing the Joint Information Environment, September 28 2013
(r) DoD Instruction 8110.01, "Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD," November 25, 2014
(s) Initial Capabilities Document (ICD) for The Joint Information Environment (JIE), v3.1, April 28, 2014
(t) DoD Directive 5000.01, "The Defense Acquisition System," May 12, 2003
(u) DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015*, as amended*
(v) CJCS Instruction 8010.01C, "Joint Community Warfighter Chief Information Officer," November 1, 2013
(w) ~~Joint Publication 1-02~~ *Office of the Chairman of the Joint Chiefs of Staff*, "~~Department of Defense~~ *DoD* Dictionary of Military and Associated Terms," current edition

(x) Memorandum of Agreement Between the Department of Defense and The Department of Homeland Security Regarding Department of Defense and U.S. Coast Guard Cooperation on Cybersecurity and Cyberspace Operations, January 19, 2017[1]

[1] *Available at https://dcms.uscg.afpims.mil/Our-Organization/Assistant-Commandant-for-C4IT-CG-6-/The-Office-of-Information-Management-CG-61/Interagency-Agreements/*

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CIO. In addition to the responsibilities in section 4 of this enclosure, the DoD CIO:

a. Serves as the DoD senior official for IRM matters.

b. Reports to and advises the Secretary and Deputy Secretary of Defense on the information resource implications of strategic planning decisions.

c. Oversees the development and maintenance of, and facilitates the use of, a DoD Enterprise Architecture (DoD EA) by major processes of DoD.

d. Oversees DoD IT investments through the development, implementation and use of the DoD IEA, which describes the future DoD IE, including cybersecurity measures and practices, as follows:

(1) DoD investments for the information enterprise are supported by regularly updated inventory of DoD-wide IT hardware, software, networks, and computing and storage centers; and

(2) The DoD CIO will establish governance mechanisms and standards to ensure compliance with and management of changes to the DoD IEA.

e. Ensures the integration and synchronization of DoD IE activities.

f. Establishes mechanisms to facilitate organizationally tiered compliance reviews for IT investments to ensure compliance with enterprise architectures, privacy requirements, and IT standards, including networks, cybersecurity, data standards, and related policy requirements. DoD CIO will act as the oversight authority for IT compliance.

g. Serves as the JIE lead and guides DoD in the delivery of the JIE.

h. Guides the DoD Components in aligning their IRM activities with the desired outcomes and goals of the JIE in accordance with the Initial Capabilities Document (ICD) for The Joint Information Environment (JIE) (Reference (s)).

i. Oversees information policy and ensures IT capability requirements are reflected in architectures and plans across DoD as a means of guaranteeing information safeguarding, sharing, visibility, trustworthiness, accessibility, and interoperability.

2. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO). Pursuant to section 11316 of Reference (c), in addition to the responsibilities in section 4, and in coordination with the DoD CIO and the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), the USD(C)/CFO establishes policies and procedures to ensure that accounting, financial, and asset management systems and other related DoD information solutions are designed, developed, and maintained, and used effectively to provide financial data reliably, consistently, quickly, and in support of programmatic investment decisions.

3 DEPUTY CHIEF MANAGEMENT OFFICER OF THE DEPARTMENT OF DEFENSE. In addition to the responsibilities in section 4, the Deputy Chief Management Officer of the Department of Defense collaborates with the DoD CIO to ensure that the business transformation and DoD IE policies and program are designed and managed to improve performance standards, economy, and efficiency.

4. OSD and DoD COMPONENT HEADS. The OSD and DoD Component heads:

a. Improve DoD operations and procedures by ensuring the application of sound business practices and compliance with this directive.

b. Oversee the evaluation and improvement of functional processes before making significant investments in IT, to:

(1) Determine whether the function that IT will support is central to, or a priority for, DoD's mission.

(2) Determine the most appropriate and cost effective service provider for IT, ensuring that DoD's cybersecurity posture is not jeopardized and critical mission capabilities are retained.

(3) Determine whether the private sector or another government agency can perform the function more effectively, ensuring that DoD's cybersecurity posture is not jeopardized and critical mission capabilities are retained.

c. Ensure that information policy and functional requirements are reflected in architectures and plans across DoD and Component-level enterprises as a means to guarantee information safeguarding, sharing, visibility, trustworthiness, accessibility, and interoperability.

d. Participate in DoD oversight processes for IT acquisition and ensure functional leadership, management, and control of these resources throughout their life cycles. Those processes conducted under the Defense Acquisition System will be in accordance with DoDD 5000.01 (Reference (t)) and DoDI 5000.02 (Reference (u)).

5. DoD COMPONENT HEADS. In addition to the responsibilities in section 4 of this enclosure, the DoD Component heads:

a. Appoint a Component CIO or senior IRM official with core knowledge, skills, abilities, and experience to carry out the IRM requirements of References (b), (c), (d), and (e), and the policies in this directive.

(1) Position the DoD Component CIO or senior IRM official to participate in the Component's strategic planning, management, and decision processes.

(2) Promote and forge a strong partnership among the Component's CIO and Comptroller, DoD Component Acquisition Executive or similar position, as well as other key senior managers and external mission partners.

(3) Designate subordinate-level CIOs or IRM officials, as needed, and ensure that the subordinate reporting mechanism goes through the Component CIO or senior IRM official.

b. Align the Component's IT investment portfolio with DoD IE policies and guidance, as required.

c. Oversee the DoD Component CIOs or senior IRM officials. The DoD Component CIOs or senior IRM officials:

(1) Have responsibilities and authorities as delegated in this directive. Military Department CIOs will have additional responsibilities as defined in Reference (b).

(2) Head an office responsible for ensuring that the component complies with, and promptly, efficiently, and effectively implements the policies and responsibilities in this directive and the requirements of References (b), (c), (d), and (e).

(3) Ensure that information policy and functional requirements are reflected in architectures and plans across the DoD and Component level enterprises as a means to guarantee information safeguarding, sharing, visibility, trustworthiness, and interoperability.

(4) Require that DoD IT is designed for interoperability and openness, and comply with established well-defined standards in order to deliver secure, device-agnostic, digital services for the best value, in accordance with References (m), (n) and (o).

(5) Ensure IT meets DoD regulations, instructions, and policies prior to installation into the DoD-wide enterprise.

(6) Establish programs to hire, train, and retain the information management, IT, and cybersecurity workforce, consistent with this directive.

(7) Participate in DoD CIO-led forums for governing the DoD IE.

(8) Ensure Component policy supports DoD-wide enterprise policy.

6. CJCS. In addition to the responsibilities in section 4 and 5 of this enclosure, the CJCS appoints a Joint Community Warfighter CIO, consistent with CJCS Instruction 8010.01C, (Reference (v)).

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CIO	chief information officer
CJCS	Chairman of the Joint Chiefs of Staff
DoD CIO	Department of Defense Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DoD IE	DoD Information Enterprise
DoD IEA	DoD Information Enterprise Architecture
IRM	information resources management
IT	information technology
JIE	joint information environment
U.S.C.	United States Code
USD(AT&L)	Under Secretary of Defense for Acquisition, Technology, and Logistics
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense

PART II. DEFINITIONS

Unless otherwise noted, these terms and their definitions are for the purposes of this directive.

cybersecurity. Defined in Reference (h).

cyberspace. Defined in ~~Joint Publication 1-02~~ *the DoD Dictionary of Military and Associated Terms* (Reference (w)).

device-agnostic. A service that is developed to work regardless of the user's device, e.g. a website that works whether viewed on a desktop computer, laptop, smartphone, media tablet or e-reader.

digital services. Include the delivery of digital information (i.e., data or content) and transactional services (e.g., online forms, benefits applications) across a variety of platforms, devices, and delivery mechanisms (e.g., websites, mobile applications, and social media)

DoD Enterprise Architecture. A federation of descriptions that provides context and rules for accomplishing the DoD mission. These descriptions are developed and maintained at the Department, Capability Area, and Component levels and collectively define the people, processes, and technology required in the "current" and "target" environments, and in the roadmap for transition to the target environment.

DoD enterprise IT service. An IT service that is offered by one DoD Component to all DoD Components.

DoD IE. The DoD information resources, assets, and processes required to achieve an information advantage and to share information across DoD and with mission partners. It includes:

The information itself and the Department's management over the information life cycle;

The processes, including risk management, associated with managing information to accomplish the DoD mission and functions;

Activities related to designing, building, populating, acquiring, managing, operating, protecting, and defending the information enterprise; and

Related information resources such as personnel, funds, equipment, and IT, including internal use software and national security systems.

DoD IEA. The description of the DoD IE including the infrastructure, communications systems and services (i.e., systems and facilities for transferring data between persons and equipment), the computing systems and services (i.e., integrated sets of components for collecting, storing, and processing data for delivering information, knowledge, and digital products for organizations and individuals to manage their operations), and the functional processes (i.e., the structured activities or tasks that produce a specific service or product) for DoD IE customers.

DoD information network. Defined in Reference (w).

information advantage. The superior position or condition derived from the ability to access, share, and collaborate securely via trusted information in order develop to more rapidly awareness and to execute decisions than an adversary while exploiting or denying an adversary's ability to do the same.

information environment. Defined in Reference (w).

information life cycle. The stages through which information passes, typically characterized as: creation or collection; processing; dissemination; use; storage; and disposition.

Internal Use Software. Software that:

Is acquired or developed to meet the entity's internal or operational needs *(intended purpose)*; and

Is a stand-alone application, or the combined software components of an IT system that can consist of multiple applications, modules, or other software components integrated and used to fulfill the entity's internal or operational needs *(software type).*

Internal Use Software can be purchased from commercial vendors "off-the-shelf", modified "off the shelf," internally developed, or contractor developed.

IRM. The process of managing information resources to accomplish agency missions and to improve agency performance, including through the reduction of the information collection burden on the public. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and IT.

IT. Any equipment or interconnected system or subsystem of equipment used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency.

This includes if the equipment is used by the executive agency directly or is used by a contractor under a contract with the executive agency that requires the use of that equipment; or of that equipment to a significant extent in the performance of a service or the furnishing of a product.

IT includes computers, ancillary equipment, software, firmware, and similar procedures, services (including support services), and related resources, but does not include any equipment acquired by a federal contractor incidental to a federal contract.

IT investment. The expenditure of IT resources to address mission delivery and management support.

An IT investment may include a project or projects for the development, modernization, enhancement, or maintenance of a single IT asset or group of IT assets with related functionality, and the subsequent operation of those assets in a production environment.

All IT investments should have a defined life cycle with start and end dates, with the end date representing the end of the currently estimated useful life of the investment, consistent with the investment's most current alternatives analysis if applicable.

When the asset(s) is essentially replaced by a new system or technology, the replacement should be reported as a new, distinct investment, with its own defined life cycle information.

IT service. 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.

mission partners. Those with whom DoD cooperates to achieve national goals, such as other departments and agencies of the U.S. Government, State and local governments, allies, coalition members, host nations and other nations, multinational organizations, non-governmental organizations, and the private sector.

National Security System. Defined in section 3552 of Reference (c).