



Department of Defense **DIRECTIVE**

NUMBER 5144.02

November 21, 2014

Incorporating Change 1, September 19, 2017

DCMO

SUBJECT: DoD Chief Information Officer (DoD CIO)

References: See Enclosure

1. **PURPOSE.** Under the authority vested in the Secretary of Defense by section 113 of Title 10, United States Code (U.S.C.) (Reference (a)), this directive:

a. Assigns the responsibilities, functions, relationships, and authorities of the DoD CIO, pursuant to sections 2222-2224 of Reference (a), section 11315 of Title 40, U.S.C. (Reference (b)), and sections 3102, 3506, and 3544 of Title 44, U.S.C. (Reference (c)).

b. Reissues DoD Directive (DoDD) 5144.02 (Reference (d)). Any reference in any law, rule, regulation, or issuance to the Assistant Secretary of Defense for Networks and Information Integration (ASD(NII)) will be deemed to be a reference to the DoD CIO, unless otherwise specified by the Secretary of Defense.

c. Authorizes the DoD CIO, as a Principal Staff Assistant (PSA) reporting directly to the Secretary of Defense, to establish DoD policy in DoD issuances within the responsibilities, functions, and authorities assigned in this directive, in accordance with DoD Instruction (DoDI) 5025.01 (Reference (e)).

2. **APPLICABILITY.** This directive applies to OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff 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 directive as the "DoD Components").

3. **RESPONSIBILITIES AND FUNCTIONS.** The DoD CIO is the PSA and senior advisor to the Secretary of Defense for information technology (IT) (including national security systems and defense business systems), information resources management (IRM) and efficiencies. The DoD CIO is responsible for all matters relating to the DoD information enterprise, including communications; spectrum management; network policy and standards; information systems;

cybersecurity; positioning, navigation, and timing (PNT) policy; and the DoD information enterprise that supports DoD command and control (C2). In this capacity, the DoD CIO:

a. Develops DoD strategy and policy on the operation and protection of all DoD IT and information systems, including development and promulgation of enterprise-wide architecture requirements and technical standards, and enforcement, operation, and maintenance of systems, interoperability, collaboration, and interface between DoD and non-DoD systems.

b. Serves as the Agency Chief Information Officer for the DoD with the responsibilities, duties, and qualifications, pursuant to section 11315 of Reference (b), and the additional responsibilities, pursuant to section 2223 of Reference (a). In performance of these duties, the DoD CIO will:

(1) Develop, maintain, and manage the implementation of a sound, secure, and integrated DoD IT architecture, ensure the interoperability of IT throughout the DoD, and prescribe IT standards, including network and cybersecurity standards that apply throughout the DoD.

(2) Ensure compliance by the Military Department chief information officers (CIOs) with their responsibilities, pursuant to section 2223 of Reference (a), and ensure compliance by all DoD Component CIOs with DoD policy under the purview of the DoD CIO.

(3) Maintain a consolidated inventory of DoD mission-critical and mission-essential information systems, identify interfaces between these systems, and develop and maintain contingency plans for responding to disruptions in the operation of any of these information systems.

(4) Monitor and evaluate the performance of DoD IT investments through applicable performance measurements and advise the Secretary of Defense, and advise relevant PSAs on investments under their purview, on whether to continue, modify, or terminate such investments.

(5) Review and provide recommendations on the DoD IT budget requests and the management of information resources.

(6) Provide for the elimination of duplicate DoD IT (including systems, applications, and infrastructure) within and between the DoD Components and interagency partners, and identify opportunities for improving IT efficiencies.

(7) Develop and maintain, in coordination with the Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L)), a process for maximizing the value of, and assessing and managing the risks related to, DoD IT acquisitions. Such a process will:

(a) Be integrated with other key DoD decision support systems and processes that support capability identification; planning, programming, budgeting and execution; and acquisitions.

(b) Provide for analyzing, selecting, monitoring, and evaluating DoD IT investments.

(c) Be performance, cost, and results based.

(8) Perform all other responsibilities and functions as required by statute, directive, or regulation pertaining to an agency CIO role.

c. Serves as the CIO for DoD with the responsibilities, pursuant to section 3506 of Reference (c), related to Federal information policy. In performance of these duties, the DoD CIO will:

(1) Advise and assist the PSAs and DoD Component heads on Federal information policy responsibilities related to issues that are under their purview.

(2) Oversee the management of information resources to reduce information collection burdens on the public; increase program efficiency and effectiveness; and improve the integrity, quality, and utility of information to all users within and outside DoD, including capabilities for ensuring dissemination of public information, public access to government information, and protections for privacy.

(3) Ensure that privacy impact assessments are conducted and reviewed, pursuant to section 208 of Public Law 107-347 (Reference (f)), prior to the initiation of new information collections or the development or procurement of any DoD IT that collects, maintains, or disseminates information.

(4) Provide guidance and oversight on the administration of DoD internet services, use of internet-based capabilities, and all internet domain-related functions.

(5) In cooperation with the Under Secretary of Defense (Comptroller)/Chief Financial Officer of the Department of Defense (USD(C)/CFO), develop a full and accurate accounting of DoD IT expenditures, related expenses, and performance metrics.

(6) Develop and maintain a strategic information resources management plan.

(7) In consultation with the Director of the Office of Management and Budget, the Administrator of General Services, and the Archivist of the United States, maintain a current and complete inventory of the agency's information resources, including directories necessary to fulfill the requirements of section 3511 and chapter 35 of Reference (c).

d. Consistent with section 932 of Public Law 113-66 (Reference (g), as implemented by Secretary of Defense memorandum (Reference (h)) and Deputy Secretary of Defense memorandum (Reference (i)), directs, manages, and provides policy guidance and oversight of the DoD cybersecurity program, which includes responsibility for the Defense Information Assurance Program, pursuant to section 2224 of Reference (a), and information security, pursuant to section 3544 of Reference (c). In the performance of these duties, the DoD CIO, in consultation and coordination with the Under Secretary of Defense for Intelligence, will provide

policy guidance to the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), regarding network operations and cybersecurity matters.

e. Ensures compliance with the requirements of National Security Directive 42 (Reference (j)) and collaborates with the DIRNSA/CHCSS on the performance of DIRNSA/CHCSS duties, pursuant to Reference (j) and Executive Order 12333 (Reference (k)), as the National Manager for National Security Telecommunications and Information Systems Security.

f. Consistent with section 171(a) of Reference (a) supports the Council on Oversight of the National Leadership Command, Control, and Communications System by providing policy guidance and oversight for the DoD information enterprise that supports DoD C2. This includes the communications, information sharing capabilities, and National Leadership Command Capabilities integrating national, strategic, operational, and tactical C2 and communications systems and programs, including support to the White House Military Office. The DoD CIO develops and oversees contingency and crisis response communications policies and planning for stabilization and reconstruction operations carried out by the DoD with emphasis given to those executed in concert with the U.S. Government interagency process, including DoD interaction with foreign nations and nongovernmental organizations.

g. Provides guidance and oversight for DoD network operations, including the standards for day-to-day defense and protection of DoD information networks; DoD IT support to military and joint missions; and resilience and reliability of information and communication networks.

h. Provides policy, oversight, and guidance for matters related to PNT. The DoD CIO:

(1) Serves as the lead for PNT policy within the DoD and the DoD representative for all interagency, domestic, and international forums related to PNT.

(2) Develops and maintains the Federal Radio Navigation Plan.

(3) Provides policy, oversight, and guidance on PNT enterprise-wide architecture and requirements.

i. Provides policy, oversight, and guidance for all DoD matters related to the electromagnetic spectrum and serves as the DoD lead for the management and use of the electromagnetic spectrum; and for electromagnetic environmental effects within DoD, nationally and internationally. The DoD CIO serves as the DoD lead for coordination, approval, and representation of DoD positions on all spectrum matters within the U.S. Government as well as in regional, national, and international spectrum management forums and organizations.

j. Provides guidance and oversight for the content of those portions of the defense business enterprise architecture that support information technology infrastructure or cybersecurity activities, pursuant to section 2222 of Reference (a).

k. Directs, manages, and provides policy guidance and oversight of the DoD Records Management Program, pursuant to chapters 31 and 33 of Reference (c).

l. Provides guidance and oversight with regard to the recruiting, retention, training, and professional development of the DoD IT and cybersecurity workforce, pursuant to section 11315 of Reference (b) and section 3544 of Reference (c). The DoD CIO will assess the requirements for agency personnel regarding IRM knowledge and skill and conduct formal training programs to educate agency program and management officials about IRM.

m. Establishes, maintains, and chairs the DoD CIO Executive Board as the single senior governance forum for DoD IT. The DoD CIO Executive Board provides advice and information to the DoD CIO on the full range of statutory and regulatory matters related to information and DoD IT.

n. Provides advice on issues related to all assigned responsibilities and functions to:

(1) The Defense Business Systems Management Committee and the Defense Business Council, as a co-chair.

(2) The Defense Acquisition Board, as a member.

(3) The Joint Requirements Oversight Council and Joint Capabilities Integration and Development System process, as an advisor, when appropriate.

(4) The Defense Space Council, as a member.

(5) The North Atlantic Treaty Organization Command, Control, and Communications Board, as the DoD representative.

(6) The Cyber Investment Management Board, as a member.

(7) The Council on the Oversight of the National Leadership Command, Control, and Communications System (NLC3S), as a member.

o. Serves as the chair of the Committee on National Security Systems, pursuant to Reference (j) and Executive Order 13231 (Reference (l)), and the co-chair of the National Security and Emergency Preparedness Communications Executive Committee, pursuant to Executive Order 13618 (Reference (m)).

p. Serves on boards, committees, and other groups pertaining to DoD CIO functional areas, and represents the Secretary and Deputy Secretary of Defense on DoD CIO matters outside DoD.

q. Participates in those planning, programming, budgeting, and execution activities that relate to assigned areas of responsibility.

r. Reviews assigned functions and responsibilities periodically to ensure that DoD Executive Agent responsibilities resident under the cognizance of the DoD CIO are in conformance with DoDD 5101.1 (Reference (n)).

s. Ensures that DoD CIO policies and programs are designed and managed to improve performance standards, economy, and efficiency, and that the Defense Information Systems Agency is attentive to the requirements of its organizational customers, both internal and external to the DoD.

t. Performs such other duties as the Secretary or Deputy Secretary of Defense may prescribe.

4. RELATIONSHIPS

a. In the performance of assigned responsibilities and functions, the DoD CIO:

(1) Reports directly to the Secretary of Defense.

(2) Exercises authority, direction, and control over the Director, Defense Information Systems Agency, in accordance with DoDD 5105.19 (Reference (o)).

(3) Coordinates and exchanges information with other OSD officials, the DoD Component heads, and Federal officials having collateral or related responsibilities and functions.

(4) Works directly with the DoD Component CIOs.

(5) Uses existing systems, facilities, and services of the DoD or other Federal agencies, when possible, to avoid duplication and to achieve maximum efficiency and economy.

(6) Collaborates with and provides integrated support to the Principal Cyber Advisor (PCA), in the office of the Under Secretary of Defense for Policy, on matters related to the PCA's assigned responsibilities, consistent with Reference (g) as implemented by References (h) and (i).

(7) Supports and informs the USD(AT&L) on all IT and cyber infrastructure acquisition matters and investment decisions, including IT-intensive software systems such as business systems, related to AT&L responsibility for management of the Defense Acquisition System and on programs for which AT&L is the Milestone Decision Authority.

b. The Secretaries of the Military Departments, through their Component CIOs, will coordinate and exchange information with the DoD CIO on:

(1) Budgets and budget requests for all DoD IT under their purview.

(2) Compliance with government and DoD standards on IT.

(3) Interoperability of DoD IT within DoD and with relevant IT systems of other Federal, State, tribal, and local government agencies, and with relevant IT systems of foreign governments.

c. The Commander of U.S. Cyber Command, through the Commander of U.S. Strategic Command, will coordinate and exchange information with the DoD CIO on all matters under the Commander's purview related to the authorities, responsibilities, and functions assigned in this directive.

d. The other PSAs and the DoD Component heads will coordinate with the DoD CIO on all matters under their purview related to the authorities, responsibilities, and functions assigned in this directive.

5. AUTHORITIES. Pursuant to the authority vested in the Secretary of Defense, and subject to his or her authority, direction, and control, and in accordance with DoD policies and issuances, the DoD CIO is hereby delegated authority to exercise, within assigned responsibilities and functional areas, all authority of the Secretary of Defense derived from statute, Executive order, or interagency agreement, except where specifically limited by statute or Executive order to the Secretary of Defense, and is hereby delegated authority to:

a. Establish, in DoDIs and directive-type memorandums (DTMs), DoD policy within the authorities and responsibilities assigned in this directive, including authority to identify collateral responsibilities of other OSD PSAs and the DoD Component heads. This authority cannot be redelegated.

(1) Such issuances must be fully coordinated, in accordance with Reference (e).

(2) In areas of assigned responsibilities and functions, the DoD CIO has authority to approve and sign other DoDIs, DoD manuals, and DTMs, in accordance with Reference (e), that implement policy approved by the Secretary or Deputy Secretary of Defense.

(3) Instructions to the Military Departments must be issued through the Secretaries of the Military Departments. Instructions to the Combatant Commands normally are communicated through the Chairman of the Joint Chiefs of Staff.

b. Obtain reports and information, in accordance with DoDI 8910.01 (Reference (p)), as necessary, to carry out assigned responsibilities and functions.

c. Communicate directly with the DoD Component heads, as necessary, to carry out assigned responsibilities and functions, including transmitting requests for advice and assistance. Communications to the Military Departments must be transmitted through the Secretaries of the Military Departments, their designees, or as otherwise provided in law or directed by the Secretary of Defense in other DoD issuances. Communications to the Commanders of the Combatant Commands normally are transmitted through the Chairman of the Joint Chiefs of Staff.

d. Communicate with other Executive Branch officials, State and local officials, representatives of non-governmental organizations, members of the public, and representatives

of foreign governments, as appropriate, in carrying out assigned responsibilities and functions. Communications with representatives of the Legislative Branch must be conducted through the Assistant Secretary of Defense for Legislative Affairs or the USD(C)/CFO, as appropriate, and be consistent with the DoD Legislative Program.

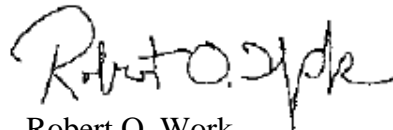
e. Communicate directly with the CIOs of the DoD Components on all matters for which the DoD CIO is assigned responsibilities herein.

f. Negotiate and conclude international agreements, in accordance with DoDD 5530.3 (Reference (q)), and other arrangements with non-Federal entities in areas of assigned responsibility, in coordination with the General Counsel of the Department of Defense.

g. Nothing in this directive shall be construed to mean that the DoD CIO has operational responsibility for cyber defensive or offensive missions.

6. RELEASABILITY. ~~UNLIMITED. This directive is approved for public release and is available on the Internet from the DoD Issuances Website at <http://www.dtic.mil/whs/directives>.~~ *Cleared for public release. This directive is available on the Directives Division Website at <http://www.esd.whs.mil/DD/>.*

7. EFFECTIVE DATE. This directive is effective ~~immediately:~~ *November 21, 2014.*



Robert O. Work
Deputy Secretary of Defense

Enclosure
References
Glossary

ENCLOSURE

REFERENCES

- (a) Title 10, United States Code
- (b) Title 40, United States Code
- (c) Title 44, United States Code
- (d) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," April 22, 2013 (hereby cancelled)
- (e) DoD Instruction 5025.01, "DoD Issuances Program," ~~June 6, 2014~~ *August 1, 2016*, as amended
- (f) Section 208 of Public Law 107-347, "The E-Government Act of 2002," December 17, 2002
- (g) Section 932 of Public Law 113-66, "The National Defense Authorization Act for Fiscal Year 2014," December 26, 2013
- (h) Deputy Secretary of Defense Memorandum, "Guidance Regarding Cyberspace Roles, Responsibilities, Functions and Governance within the Department of Defense," June 9, 2014
- (i) Secretary of Defense Memorandum, "Designation of the DoD Principal Cyber Advisor," July 17, 2014
- (j) National Security Directive 42, "National Policy for the Security of National Security Telecommunications and Information Systems," July 5, 1990
- (k) Executive Order 12333, "United States Intelligence Activities," as amended
- (l) Executive Order 13231, "Critical Infrastructure Protection in the Information Age," October 16, 2001, as amended
- (m) Executive Order 13618, "Assignment of National Security and Emergency Preparedness Communications Functions," July 6, 2012
- (n) DoD Directive 5101.1, "DoD Executive Agent," September 3, 2002, as amended
- (o) DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," July 25, 2006
- (p) DoD Instruction 8910.01, "Information Collection and Reporting," May 19, 2014
- (q) DoD Directive 5530.3, "International Agreements," June 11, 1987, as amended
- (r) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014
- (s) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (*DoD IE*)," ~~February 10, 2009~~ *March 17, 2016, as amended*
- (t) DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities," September 11, 2012

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ASD(NII)	Assistant Secretary of Defense for Networks and Information Integration
C2	command and control
CIO	chief information officer
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
DTM	directive-type memorandum
IRM	information resources management
IT	information technology
PCA	Principal Cyber Advisor
PNT	positioning, navigation, and timing
PSA	Principal Staff Assistant
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 purpose of this directive.

cybersecurity. Defined in DoDI 8500.01 (Reference (r)).

DoD information enterprise. Defined in DoDI 8000.01 (Reference (s)).

DoD information. Defined in Reference (r).

DoD IT. Defined in Reference (r).

internet-based capabilities. Defined in DoDI 8550.01 (Reference (t)).

IRM. Defined in section 3502 of Reference (c).

IT. Defined in section 11101 of Reference (b).

national security systems. Defined in section 3542 of Reference (c).