DoD Directive 8140.01

Cyberspace Workforce Management

Originating Component:	Office of the DoD Chief Information Officer
Effective:	October 5, 2020
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Directive 8140.01, "Cyberspace Workforce Management," August 11, 2015, as amended
Approved by:	David L. Norquist, Deputy Secretary of Defense

Purpose: In accordance with Sections 303 and 304 of Public Law 114-113, also known and referred to in this issuance as the Federal Cybersecurity Workforce Assessment Act of 2015, this issuance:

- Authorizes establishment of a DoD Cyberspace Workforce Management Board (CWMB) as the governing body to ensure that the requirements of this issuance are met.
- Establishes the DoD Cyberspace Workforce Framework (DCWF) as the authoritative reference for the identification, tracking, and reporting of DoD cyberspace positions and foundation for developing enterprise baseline cyberspace workforce qualifications.
- Unifies the overall cyberspace workforce and establishes specific workforce elements (e.g., information technology (IT), cybersecurity, cyberspace effects, intelligence, and enablers) to align and manage the cyberspace workforce under the CWMB.

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

This issuance applies to the OSD, the Military Departments (including the Coast Guard at all times, including when it is a Service in the Department of Homeland Security by agreement with that Department), 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 issuance as the "DoD Components").

1.2. POLICY.

a. The DoD maintains a total force management perspective to provide qualified cyberspace government civilian and military personnel to identified and authorized positions, augmented where appropriate by contracted services support. These personnel function as an integrated workforce with complementary skill sets to provide an agile, flexible response to DoD requirements.

b. The appropriate mix of military and government civilian positions and contracted support designated to perform cyberspace work roles is determined in accordance with DoD Instruction (DoDI) 1100.22.

c. Civilian and military personnel performing cyberspace work roles must meet qualification standards established in DoD cyberspace workforce policy, in addition to other applicable workforce qualification and training requirements (e.g., acquisition, intelligence, communications). These requirements should not be construed to modify, replace, or conflict with General Schedule occupational qualification requirements established by the Office of Personnel Management.

d. DoD Component compliance with this issuance is monitored via authoritative manpower and personnel systems as an element of mission readiness; as appropriate and as a management review item.

e. Nothing in this issuance:

(1) Replaces or infringes on the responsibilities, functions, or authorities of the OSD or DoD Component heads, as prescribed by law or Executive order, assigned in chartering DoD directives (DoDDs), detailed in other DoD issuances or, as applicable, in Director of National Intelligence policy issuances.

(2) Infringes on the DoD Office of the Inspector General's statutory independence and authority as articulated in Public Law 95-452, as amended. In the event of any conflict between this issuance and the DoD Office of the Inspector General's statutory independence and authority, Public Law 95-452 takes precedence.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICER (DOD CIO).

In addition to the responsibilities in Paragraph 2.10., the DoD CIO:

a. Oversees the management of DoD IT, cybersecurity, and cyberspace enabler workforce elements of the DoD cyberspace workforce in accordance with DoDDs 5144.02 and 8000.01.

b. Recommends, in collaboration with the DoD Component heads, cyberspace workforce management requirements and personnel qualification standards for positions and personnel required to perform IT, cybersecurity, and enabler work roles to the CWMB for approval, in accordance with DoDDs 1100.4, 5144.02, and 8000.01.

c. Serves as a standing member of the CWMB in accordance with the CWMB charter.

d. Collaborates with the Under Secretary of Defense for Personnel and Readiness (USD(P&R)) and the DoD Component heads to establish metrics to monitor and validate compliance with this issuance.

e. Establishes, in coordination with the CJCS, academic programs at the National Defense University to educate leaders in IT, information resources management, and cybersecurity requirements and capabilities.

f. Collaborates with appropriate stakeholders to develop requirements and provide guidance and oversight to the DoD Cyber Crime Center (DC3) in support of training and qualification development specialized cyber training, digital forensics examiners, cyber analysis and cybersecurity in accordance with DoDD 5505.13E.

g. Serves as the Office of Primary Responsibility for DoD IT, cybersecurity, and cyberspace enabler work roles.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY.

Under the authority, direction, and control of the DoD CIO, and in addition to the responsibilities in Paragraph 2.10., the Director, Defense Information Systems Agency:

a. Provides DoD Components with training materials, content, products, assessment tools, and methodologies related to DoD IT and cybersecurity policies, concepts, procedures, tools, techniques, and systems.

b. Provides shareable methodology and tools, including timelines and implementation guidance, to DoD Components to establish and measure effectiveness of training programs.

2.3. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT.

In addition to the responsibilities in Paragraph 2.10., the Under Secretary of Defense for Acquisition and Sustainment:

a. Recommends, in collaboration with the DoD Component heads, acquisition qualification requirements for work roles responsible for acquisition of DoD systems and cyberspace capabilities to the CWMB for approval.

b. Ensures personnel performing cyberspace work roles within the DoD information network system development lifecycle processes are qualified in accordance with DoD cyberspace workforce policy.

c. Provides guidance and oversight to the Defense Acquisition Workforce to incorporate the requirements of this issuance into contracts.

d. In coordination with the President of the Defense Acquisition University, ensures that cyberspace work role requirements are integrated into appropriate acquisition training and development curriculum.

2.4. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING.

In addition to the responsibilities in Paragraph 2.10., the Under Secretary of Defense for Research and Engineering:

a. Recommends, in collaboration with the DoD Component heads, acquisition qualification requirements for work roles responsible for research and development of DoD systems and cyberspace capabilities to the CWMB for approval.

b. Ensures personnel performing cyberspace work roles within the DoD information systems life-cycle development processes are qualified in accordance with DoD cyberspace workforce policy.

c. In coordination with the President of the Defense Acquisition University, ensures that cyberspace work role requirements are integrated into appropriate acquisition training and development curriculum.

2.5. USD(P&R).

In addition to the responsibilities in Paragraph 2.10., the USD(P&R):

a. Establishes policy guidance to support military cyberspace training requirements in accordance with DoDD 1322.18.

b. Provides DoD Components with access to systems collecting required cyberspace workforce manpower and personnel data required by DoD cyberspace workforce policy. For

required information not currently collected, develop data elements and direct collection in authoritative manpower and personnel systems.

c. Serves as standing member of the CWMB in accordance with the CWMB charter.

d. Provides DoD Components with manpower and Total Force policies for determining requirements and manpower mix.

e. Facilitates labor-management obligations in accordance with Volume 711 of DoDI 1400.25.

2.6. UNDER SECRETARY OF DEFENSE FOR INTELLIGENCE AND SECURITY (USD(I&S)).

In addition to the responsibilities in Paragraph 2.10., the USD(I&S):

a. Establishes and maintains workforce management requirements, qualification standards, and certification programs for intelligence, counterintelligence, security, law enforcement, sensitive activities, and other related positions and personnel required to operate in or support the cyberspace domain. This is done in coordination with the Defense intelligence, counterintelligence, and law enforcement agencies, the Joint Staff, the Office of the USD(P&R), and the Military Departments.

b. Establishes and maintains, in coordination with the DoD CIO, appropriate workforce management requirements and personnel qualification standards for digital forensics to support DC3 curriculum development in accordance with DoDD 5505.13E.

c. Serves as a standing member of the CWMB.

d. Implements this issuance for personnel who support DoD intelligence, security, and law enforcement missions in the cyberspace domain, and acts as the Office of Primary Responsibility for work roles and associated qualification standards for the intelligence elements of the DoD cyberspace workforce.

2.7. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE.

Under the authority, direction, and control of the USD(I&S), and in addition to the responsibilities in Paragraph 2.10., the Director, National Security Agency/Chief, Central Security Service:

a. Oversees development and maintenance of standards for cryptologic work roles related to cyberspace operations, training, and personnel certifications in accordance with DoDIs 3115.11 and 3305.09.

b. Develops and provides appropriate training and education standards for DoD personnel who perform cryptologic work roles related to cyberspace operations.

2.8. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)).

In addition to the responsibilities in Paragraph 2.10., the USD(P):

a. Coordinates and maintains a cyberspace strategy and advises on implementing that strategy in accordance with DoDD 5111.01.

b. Serves as a standing member of the CWMB.

2.9. ASSISTANT SECRETARY OF DEFENSE FOR HOMELAND DEFENSE AND GLOBAL SECURITY.

Under the authority, direction, and control of the USD(P) and in addition to the responsibilities in Paragraph 2.10., the Assistant Secretary of Defense for Homeland Defense and Global Security, in his or her role as the Principal Cyber Advisor:

a. Recommends, in collaboration with the DoD Component heads, workforce management requirements and qualification standards for positions and personnel required to perform cyberspace effects work roles to the CWMB for approval.

b. Collaborates with the DoD CIO, the USD(P&R), the USD(I&S), the Secretaries of the Military Departments, the Commandant of the United States Coast Guard, and the CJCS to establish metrics for the cyberspace effects workforce to monitor and validate compliance as an element of mission readiness.

c. Serves as the Office of Primary Responsibility for cyberspace effects work roles.

d. Serves as a standing member of the CWMB in accordance with the CWMB charter.

2.10. OSD AND DOD COMPONENT HEADS.

The OSD and DoD Component heads:

a. Establish, resource, implement, and assess cyberspace workforce management programs for all DoD Component personnel in accordance with this issuance.

b. Identify total manpower required to perform cyberspace work roles in authoritative manpower and personnel systems in accordance with the Federal Cybersecurity Workforce Assessment Act of 2015.

c. Identify, document, track, and report qualifications for military, DoD civilian, and contractor support personnel who perform cyberspace work roles in accordance with DoDD 8000.01, DoDI 1336.05, Volume 4 of DoDI 1444.02, and Volume 1 of DoD Manual 7730.54.

d. Specify workforce qualification requirements in contracts that include the acquisition of personnel and services to perform cyberspace work roles. Contractor personnel performing such work roles must have their qualifications documented.

e. Through their DoD Component contracting officials, apply updated qualification standards, according to Defense Federal Acquisition Regulation Supplement Subpart 239.71, for contractors performing cyberspace work roles.

f. Require personnel who perform cyberspace work roles to meet qualification requirements established pursuant to this issuance.

g. Provide appropriate training for personnel who conduct assessments and inspections to ensure DoD Components have a compliant cyberspace workforce management program, including the verification of workforce qualifications.

h. Train students on the cyberspace domain and cyberspace operations considerations in professional military education.

i. Coordinate with the DoD intelligence, counterintelligence, and law enforcement agencies, the Joint Staff, Military Departments, and the Offices of the USD(P&R) and DoD CIO on the workforce management requirements, qualification standards, and certification programs for positions and personnel required to operate in or support the cyberspace domain.

j. Identify, establish, resource, implement, sustain, and assess additional Component-specific cyberspace work role training, qualification, and standards for the Component cyberspace workforce.

k. Provide access to current techniques, requirements, and knowledge resources to support developing personnel performing any cyberspace work role.

l. In conjunction with Joint Staff and the Combatant Commands, determine operational employment of the cyberspace workforce to address mission requirements.

m. Adhere to all labor-management obligations in accordance with Volume 711 of DoDI 1400.25.

n. Use the DCWF as the DoD authoritative reference for identifying, tracking, and reporting on cyberspace positions

o. Include compliance with the requirements of this issuance in DoD and DoD Component-level inspection programs and readiness reporting.

2.11. SECRETARIES OF THE MILITARY DEPARTMENTS AND COMMANDANT OF THE UNITED STATES COAST GUARD.

In addition to the responsibilities in Paragraph 2.10., the Secretaries of the Military Departments and the Commandant of the United States Coast Guard designate a representative to act as a standing member of the CWMB, in accordance with CWMB charter requirements.

2.12. SECRETARY OF THE AIR FORCE.

As the DoD Executive Agent for the DC3 and for digital/multimedia forensics within the DoD Forensic Enterprise, in accordance with DoDDs 5505.13E and 5205.15E; and in addition to the responsibilities in Paragraphs 2.10. and 2.11., the Secretary of the Air Force, through the Director, DC3:

a. Supports development of standards for digital forensics personnel training and qualifications.

b. Coordinates with the DoD CIO, the USD(I&S), and the Secretaries of the other Military Departments to integrate appropriate training and education for DoD personnel who perform cyberspace investigations, digital forensics, and cyberspace analysis.

2.13. CJCS.

In addition to the responsibilities in Paragraph 2.10., the CJCS:

a. Facilitates joint force development consistent with the overall responsibility of the CJCS to integrate cyberspace operations. This includes applications to:

(1) Strategy, policy, doctrine, and joint concepts of operations.

(2) Education, training, and exercises for DoD joint and combined operations.

b. Coordinates with the DoD CIO, the USD(P), the USD(I&S), and the Secretaries of the Military Departments on qualification standards for all cyberspace work roles, as appropriate.

c. Serves as a standing member of the CWMB.

d. Identifies, documents, and tracks joint positions and personnel assigned to cyberspace workforce positions in joint manpower and personnel system(s).

e. Facilitates coordination of work role requirements assigned to positions at Combatant Commands and their supporting Military Services when operating in the cyberspace domain.

2.14. COMMANDER, UNITED STATES CYBER COMMAND.

In addition to the responsibilities in Paragraph 2.10., the Commander, United States Cyber Command:

a. Coordinates with the DoD CIO, the Principal Cyber Advisor, the USD(I&S), the CJCS, the Secretaries of the Military Departments, and the Commandant of the United States Coast Guard on qualification standards for all cyberspace work roles, as appropriate, to ensure enterprise baseline standards support mission force qualifications.

b. Ensures assigned joint forces are trained, certified, and interoperable with other forces.

c. Develops and maintains orders and instructions necessary to provision, train, and operate the DoD Cyber Operations Forces (COF).

(1) According to the DoD COF definition, there are five operational groups specifically categorized as the DoD COF including cyber mission forces, United States Cyber Command subordinate Command elements, DoD Component Network Operations Centers and Cyber Security Service Providers, special capability providers, and specially designated units.

(2) According to the DoD COF definition, there are five operational groups not categorized as DoD COF including business function elements, service retained forces, Joint Cyber Centers, Intelligence units and personnel, and Commander, United States Special Operations Command-assigned forces.

d. Conducts and supports joint training exercises.

e. Develops recommendations to the CJCS regarding strategy, doctrine, tactics, techniques, and procedures for the joint employment of the COF.

f. Identifies and recommends global joint sourcing solutions to the CJCS in coordination with the Military Services and other Combatant Commands, and supervises the implementation of sourcing decisions.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CJCS	Chairman of the Joint Chiefs of Staff
COF	cyber operations forces
CWMB	Cyberspace Workforce Management Board
DC3	DoD Cyber Crime Center
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
IT	information technology
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(P)	Under Secretary of Defense for Policy
USD(P&R)	Under Secretary of Defense for Personnel and Readiness

G.2. DEFINITIONS.

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

TERM	DEFINITION
certification	Defined in the August 13, 2008 Office of Personnel Management Memorandum.
cyber operations force	Units organized, trained, and equipped to conduct offensive cyberspace operations (OCO), defensive cyberspace operations (DCO), and DoD Information Network operations.
cybersecurity	Defined in Committee on National Security Systems Instruction No. 4009.
cybersecurity workforce	Personnel who secure, defend, and preserve data, networks, net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place, and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities.
cyberspace	Defined in the DoD Dictionary of Military and Associated Terms.

TERM	DEFINITION
cyberspace effects workforce	Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.
cyberspace enabler workforce	Personnel who perform work roles to support or facilitate the functions of cyber IT, cybersecurity, cyberspace effects, or intelligence workforce (cyberspace) work roles. This includes actions to support acquisition, training and leadership activities.
cyberspace operations	Defined in Committee on National Security Systems Instruction No. 4009.
cyberspace workforce	Personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. It is comprised of personnel assigned to the following workforce elements: IT, cybersecurity, cyberspace effects, intelligence workforce (cyberspace), cybersecurity, IT, portions of the Intelligence workforces and cyberspace enablers.
information system	Defined in Committee on National Security Systems Instruction No. 4009.
intelligence workforce (cyberspace)	Personnel who collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyberspace programs, intentions, capabilities, research and development, and operational activities.
IT	Defined in Committee on National Security Systems Instruction No. 4009.
IT workforce	Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.
total force	Defined in DoDD 5124.02.
work role	Describes a distinct set of activities and attributes needed for the successful execution of work. A person may perform one or more work roles within their assigned position, billet, or contracted service requirement.

REFERENCES

Committee on National Security Systems Instruction No. 4009, "Committee on National Security Systems (CNSS) Glossary," April 2015

Defense Federal Acquisition Regulation Supplement, Subpart 239.71, "Security and Privacy for Computer Systems," current edition

DoD Cyberspace Workforce Management Board Charter, current edition[1]

DoD Directive 1100.4, "Guidance for Manpower Management," February 12, 2005

DoD Directive 1322.18, "Military Training," October 3, 2019

DoD Directive 5111.01, "Under Secretary of Defense for Policy (USD(P))," June 23, 2020

DoD Directive 5124.02, "Under Secretary of Defense for Personnel and Readiness (USD(P&R))," June 23, 2008

DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014, as amended

DoD Directive 5205.15E, "DoD Forensic Enterprise (DFE)," April 26, 2011, as amended

DoD Directive 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010, as amended

DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 17, 2016, as amended

DoD Instruction 1100.22, "Policy and Procedures for Determining Workforce Mix," April 12, 2010, as amended

DoD Instruction 1336.05, "Automated Extract of Active Duty Military Personnel Records," July 28, 2009, as amended

DoD Instruction 1400.25, Volume 711, "DoD Civilian Personnel Management System: Labor-Management Relations," February 26, 2020

DoD Instruction 1444.02, Volume 4, "Data Submission Requirements for DoD Civilian Personnel: Workforce and Address Dynamic Records," November 5, 2013, as amended

DoD Instruction 3115.11, "DoD Intelligence Human Capital Management Operations," January 22, 2009, as amended

DoD Instruction 3305.09, "DoD Cryptologic Training," June 13, 2013, as amended

DoD Manual 7730.54, Volume 1, "Reserve Components Common Personnel Data System (RCCPDS): Reporting Procedures," May 25, 2011, as amended

Office of Personnel Management Memorandum for Chief Human Capital Officers, "Fact Sheet on Certification and Certificate Programs," August 13, 2008

Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition

[1] DoD Cyberspace Workforce Management Board Charter is available at https://rmfks.osd.mil/rmf/collaboration/Component%20Workspaces/DoDCyberWorkforce/Pages/default.aspx

Public Law 95-452, "The Inspector General Act of 1978," October 12, 1978 as amended

Public Law 114-113, Sections 303 and 304, "Federal Cybersecurity Workforce Assessment Act of 2015," December 18, 2015