Department of Defense
DIRECTIVE

NUMBER 8140.01
August 11, 2015
Incorporating Change 1, July 31, 2017

DoD CIO

SUBJECT: Cyberspace Workforce Management

References: See Enclosure 1

1. PURPOSE. This directive:

a. Reissues and renumbers DoD Directive (DoDD) 8570.01 (Reference (a)) to update and expand established policies and assigned responsibilities for managing the DoD cyberspace workforce.

b. Authorizes establishment of a DoD cyberspace workforce management council to ensure that the requirements of this directive are met. The council will be comprised of representatives from the Offices of the DoD Chief Information Officer (DoD CIO), Under Secretary of Defense for Personnel and Readiness (USD(P&R)), Under Secretary of Defense for Policy (USD(P)), Under Secretary of Defense for Intelligence (USD(I)), the Joint Staff, the Director, National Security Agency/Chief, Central Security Service (DIRNSA/CHCSS), and other DoD Components.

c. Unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements. This directive does **not** address operational employment of the work roles. Operational employment of the cyberspace workforce will be determined by the Joint Staff, Combatant Commands, and other DoD Components to address mission requirements.

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 (IG DoD), 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").

b. The United States Coast Guard. The United States Coast Guard will adhere to DoD cybersecurity requirements, standards, and policies in this instruction in accordance with the direction in Paragraph 4a of the Memorandum of Agreement Between the Department of Defense and the Department of Homeland Security (Reference (b)).

3. POLICY. It is DoD policy that:

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 (Reference (c)).

c. Civilian, military, and contracted support personnel assigned to perform cyberspace work roles must meet qualification standards established in supporting issuances, in addition to other existing workforce qualification and training requirements assigned to billets and position requirements (e.g., acquisition, intelligence, communications). DoD Component contracting officials apply subpart 239.71 of the Defense Federal Acquisition Regulation Supplement (Reference (d)) for contracted support designated to perform cyberspace workforce work roles.

d. DoD Component compliance with this directive is monitored via authoritative manpower and personnel systems as an element of mission readiness and as a management review item. Compliance with requirements of this directive must be included in DoD and DoD Component-level inspection programs and readiness reporting.

e. Nothing in this directive replaces or infringes the responsibilities, functions, or authorities of the DoD Component heads or other OSD officials as prescribed by law or Executive order, assigned in chartering DoDDs, or detailed in other DoD policy issuances or, as applicable, in Director of National Intelligence policy issuances.

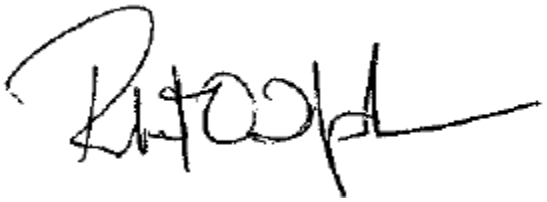
f. All authorized users of DoD IT receive initial cybersecurity and information assurance awareness orientation as a condition of access, and thereafter must complete annual cybersecurity and information assurance refresher awareness.

4. RESPONSIBILITIES. See Enclosure 2.

5. RELEASABILITY. **Cleared for public release**. This directive is available on the Directives Division Website at https://www.esd.whs.mil/DD.

6. SUMMARY OF CHANGE 1. The changes to this issuance are administrative and update references for accuracy.

7. EFFECTIVE DATE. This directive is effective August 11, 2015.



Robert O. Work
Deputy Secretary of Defense

Enclosures
1. References
2. Responsibilities

Glossary

ENCLOSURE 1

REFERENCES

(a) DoD Directive 8570.01, "Information Assurance (IA) Training, Certification, and Workforce Management," August 15, 2004, as amended (hereby cancelled)
(b) 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]
(c) DoD Instruction 1100.22, "Policy and Procedures for Determining Workforce Mix," April 12, 2010
(d) Defense Federal Acquisition Regulation Supplement, Subpart 239.71, "Security and Privacy for Computer Systems," June 21, 2010, as amended
(e) DoD Directive 5144.02, "DoD Chief Information Officer (DoD CIO)," November 21, 2014
(f) DoD Directive 8000.01, "Management of the Department of Defense Information Enterprise (DoD IE)," March 13, 2016
(g) DoD Directive 1100.4, "Guidance for Manpower Management," February 12, 2005
(h) DoD Manual 8910.01, Volume 1, "DoD Information Collections Manual: Procedures for DoD Internal Information Collections," June 30, 2014, as amended
(i) U.S. Office of Personnel Management Memorandum for Chief Human Capital Officers, "Fact Sheet on Certification and Certificate Programs," August 13, 2008
(j) DoD Directive 5505.13E, "DoD Executive Agent (EA) for the DoD Cyber Crime Center (DC3)," March 1, 2010
(k) Section 1702 of Title 10, United States Code
(l) DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005, as amended
(m) DoD Directive 1322.18, "Military Training," January 13, 2009, as amended
(n) DoD Instruction 3115.11, "DoD Intelligence Human Capital Management Operations," January 22, 2009, as amended
(o) DoD Instruction 3305.09, "DoD Cryptologic Training," June 13, 2013
(p) DoD Directive 5111.1, "Under Secretary of Defense for Policy (USD(P))," December 8, 1999
(q) DoD Instruction 1336.05, "Automated Extract of Active Duty Military Personnel Records," July 28, 2009, as amended
(r) DoD Manual 7730.54, Volume 1, "Reserve Components Common Personnel Data System (RCCPDS): Reporting Procedures," May 25, 2011, as amended
(s) DoD Instruction 1444.02, Volume 4, "Data Submission Requirements for DoD Civilian Personnel: Workforce and Address Dynamic Records," November 5, 2013
(t) DoD Directive 7730.65, "Department of Defense Readiness Reporting System (DRRS)," May 11, 2015
(u) DoD Instruction 8500.01, "Cybersecurity," March 14, 2014

[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/

(v) Office of the Chairman of the Joint Chiefs of Staff, "DoD Dictionary of Military and Associated Terms," current edition
(w) Committee on National Security Systems Instruction Number 4009, “National Information Assurance (IA) Glossary,” April 26, 2010, as amended
(x) DoD Directive 5124.02, “Under Secretary of Defense for Personnel and Readiness (USD(P&R)),” June 23, 2008

ENCLOSURE 2

RESPONSIBILITIES

1. DoD CIO. In addition to responsibilities in section 9 of this enclosure, the DoD CIO:

a. Oversees management of DoD cyberspace IT and cybersecurity workforce elements of the DoD cyberspace workforce in accordance with DoDDs 5144.02 (Reference (e)) and 8000.01 (Reference (f)).

b. In collaboration with the USD(P&R) and DoD Component heads, establishes appropriate workforce management requirements and personnel qualifications standards for the DoD cybersecurity and cyberspace IT workforce(s) pursuant to References (e) and (f) and in accordance with DoDD 1100.4 (Reference (g)).

c. Collaborates with the USD(P&R), USD(P), USD(I), Secretaries of the Military Departments, CJCS, and the DIRNSA/CHCSS to establish a DoD cyberspace workforce management council.

d. Collaborates with the USD(P&R) and the DoD Component heads to establish metrics to monitor and validate compliance with this directive as an element of mission readiness in accordance with the procedures of Volume 1 of DoD Manual 8910.01 (Reference (h)).

e. Establishes criteria and processes for selecting certification programs as defined by the Office of Personnel Management Memorandum (Reference (i)) for the cybersecurity and cyberspace IT workforces in accordance with References (e) and (f).

f. In coordination with the CJCS, establishes academic programs at the National Defense University's Information Resources Management College to educate leaders in IT, information resources management, and cybersecurity requirements and capabilities.

g. Collaborates with appropriate stakeholders to develop requirements and provide guidance and oversight to DoD Cyber Crime Center (DC3) in support of training and qualification development for digital forensics in accordance with DoDD 5505.13E (Reference (j)).

2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). In addition to responsibilities in section 9 of this enclosure and under the authority, direction, and control of the DoD CIO, the Director, DISA:

a. Provides access to current techniques, requirements, and knowledge resources to support development of personnel performing work roles in DoD cybersecurity and cyberspace IT workforces.

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

c. Provides shareable methodology and tools, to include timeline and implementation guidance, to DoD Components to establish and measure effectiveness of cybersecurity awareness and training programs.

d. Incorporates cyberspace IT workforce and cybersecurity workforce qualification and management requirements into DoD and DoD Component inspection programs.

3. USD(AT&L). In addition to responsibilities in section 9 of this enclosure, the USD(AT&L):

a. In coordination with the DoD CIO and applicable DoD Component heads, establishes the acquisition qualification requirements for work roles responsible for research, development, and acquisition of DoD IT, information systems, platform IT, and cyberspace capabilities.

b. Supports integration of qualified cyberspace workforce personnel into DoD information systems lifecycle development processes.

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

d. Establishes policies and procedures, in coordination with the USD(P&R), DoD CIO, USD(I), USD(P), Secretaries of the Military Departments, and the CJCS, for the effective management of the acquisition, technology, and logistics workforce supporting DoD cyberspace programs in accordance with section 1702 of Title 10, United States Code (Reference (k)) and DoDD 5134.01 (Reference (l)).

e. Provides direction and oversight of the Defense Acquisition University to ensure that cybersecurity work role requirements are integrated into training, courses, and curriculum.

4. USD(P&R). In addition to the responsibilities in section 9 of this enclosure, the USD(P&R):

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

b. Provides, as appropriate, DoD Components with access to systems that identify and track personnel, manpower, training, education, and qualifications to support cyberspace workforce lifecycle management.

c. Supports the DoD Components in determining requirements for DoD military and civilian manpower in accordance with Reference (g) and contract support needed to perform cyberspace missions.

d. Collaborates with the DoD CIO, USD(P), USD(I), Secretaries of the Military Departments, CJCS, and the DIRNSA/CHCSS to establish a DoD cyberspace workforce management council.

e. Supports identification of DoD Component cyberspace workforce reporting requirements.

5. USD(I). In addition to the responsibilities in section 9 of this enclosure, the USD(I):

a. Establishes and maintains workforce management requirements, qualification standards, and certification programs for intelligence, counterintelligence (CI), security, law enforcement (LE), sensitive activities, and other related positions and personnel required to operate in or support the cyberspace domain. This is done in coordination with Defense intelligence, CI and LE 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 Reference (j).

c. Implements this directive for personnel who support DoD intelligence, security, and LE missions in the cyberspace domain.

d. Collaborates with the DoD CIO, USD(P&R), USD(P), Secretaries of the Military Departments, CJCS, and the DIRNSA/CHCSS to establish a DoD cyberspace workforce management council.

6. DIRNSA/CHCSS. In addition to the responsibilities in section 9 of this enclosure and under the authority, direction, and control of USD(I), the DIRNSA/CHCSS:

a. Oversees development and maintenance of standards for cryptologic work roles related to cyberspace operations, training, and personnel certifications in accordance with DoDI 3115.11 (Reference (n)) and DoDI 3305.09 (Reference (o)).

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

c. Collaborates with the DoD CIO, USD(P&R), USD(P), USD(I), Secretaries of the Military Departments, and the CJCS to establish a DoD cyberspace workforce management council.

7. USD(P). In addition to the responsibilities in section 9 of this enclosure, the USD(P):

a. Collaborates with the DoD CIO, USD(P&R), USD(I), Secretaries of the Military Departments, CJCS, and the DIRNSA/CHCSS to establish a DoD cyberspace workforce management council.

b. Coordinates and maintains a cyberspace strategy and advises on implementing that strategy in accordance with DoDD 5111.1 (Reference (p)).

c. Establishes and maintains, in coordination with the Joint Staff and Military Departments, workforce management requirements and qualification standards for positions and personnel required to perform cyberspace effects work roles.

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

8. IG DoD. In addition to the responsibilities in section 9 of this enclosure, the IG DoD, at his or her discretion, establishes and leverages qualification standards for personnel supporting and performing audits and inspections in the cyberspace domain.

9. 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 directive.

b. In addition to DoD mandated cybersecurity awareness training, provide DoD Component-specific cybersecurity orientation, training, awareness, and reinforcement programs to authorized users of information systems.

c. Identify total manpower required to perform cyberspace work roles in manpower databases in accordance with Reference (g).

d. Identify, document, track, and report qualifications for military, DoD civilian, and contractor support personnel who perform cyberspace work roles using authoritative personnel databases in accordance with Reference (g) and DoDI 1336.05, Volume 1 of DoD 7730.54-M, and Volume 4 of DoDI 1444.02 (References (q), (r), and (s)).

e. 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 in an authoritative verification system(s) in accordance with Reference (g).

f. Require personnel who perform cyberspace work roles to meet qualification requirements in accordance with issuances supporting this directive.

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

h. Incorporate the cyberspace domain and operations in professional military education.

i. Coordinate with Defense intelligence, CI, and LE 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. Include unit-based reporting of cyberspace workforce readiness status in the Defense Readiness Reporting System in accordance with DoDD 7730.65 (Reference (t)).

10. SECRETARIES OF THE MILITARY DEPARTMENTS. In addition to the responsibilities in section 9 of this enclosure, the Secretaries of the Military Departments will collaborate with the DoD CIO, USD(P&R), USD(I), USD(P), CJCS, and the DIRNSA/CHCSS to establish a DoD cyberspace workforce management council.

11. SECRETARY OF THE AIR FORCE. In his or her capacity as the DoD Executive Agent for the DC3 in accordance with Reference (k), and in addition to responsibilities in sections 9 and 10 of this enclosure, 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, USD(I), and Secretaries of the other Military Departments to integrate appropriate training and education for DoD personnel who perform digital forensics.

12. CJCS. In addition to the responsibilities in section 9 of this enclosure, the CJCS:

a. Facilitates joint force development consistent with the overall responsibility of the CJCS to integrate cyberspace capabilities. Includes applications into strategy, policy, doctrine, concepts of operations, education, training, and exercises for DoD joint and combined operations in the cyberspace domain.

b. Coordinates with the DoD CIO, USD(P), USD(I), and the Secretaries of the Military Departments on qualifications requirements for cyberspace work roles, as appropriate.

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

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

e. Collaborates with the DoD CIO, USD(P&R), USD(I), USD(P), Secretaries of the Military Departments and the DIRNSA/CHCSS to establish a DoD cyberspace workforce management council.

f. Provides access to current techniques, requirements, and knowledge resources to support development of personnel performing work roles in DoD cyberspace effects, cybersecurity, and cyberspace IT workforces.

g. Provides training materials, content, products, assessment tools, and methodologies related to DoD cyberspace effects, cybersecurity, and cyberspace IT policies, concepts, procedures, tools, techniques, and systems.

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

CI	counterintelligence
CJCS	Chairman of the Joint Chiefs of Staff
DC3	DoD Cyber Crime Center
DIRNSA/CHCSS	Director, National Security Agency/Chief, Central Security Service
DISA	Defense Information Systems Agency
DoD CIO	DoD Chief Information Officer
DoDD	DoD Directive
DoDI	DoD Instruction
IG DoD	Inspector General Department of Defense
IT	information technology
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

PART II. DEFINITIONS

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

authorized user. Defined in DoDI 8500.01 (Reference (u)).

certification. Defined in Reference (i).

cybersecurity. Defined in Reference (u).

cyberspace. Defined in the DoD Dictionary of Military and Associated Terms (Reference (v)).

cyberspace operations. Defined in Reference (v).

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 areas of cyberspace effects, cybersecurity, cyberspace IT, and portions of the Intelligence workforces:

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 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 IT workforce. Personnel who design, build, configure, operate, and maintain IT, networks, and capabilities. This includes actions to prioritize portfolio investments; architect, engineer, acquire, implement, evaluate, and dispose of IT as well as information resource management; and the management, storage, transmission, and display of data and information.

intelligence workforce (cyberspace). Personnel who collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities.

information assurance. Defined in Reference (v).

information system. Defined in Reference (w).

IT. Defined in Reference (f).

platform IT. Defined in Reference (u).

total force. Defined in Reference (x).

work role. The knowledge, skills, and abilities that a person must have to perform a set of functions or tasks.