DoD Instruction 8410.02

Support to DoD Information Network Operations

Originating Component:	Office of the DoD Chief Information Officer
Effective:	December 8, 2021
Releasability:	Cleared for public release. Available on the Directives Division Website at https://www.esd.whs.mil/DD/.
Reissues and Cancels:	DoD Instruction 8410.02, "NetOps for the Global Information Grid (GIG)," December 19, 2008
Approved by:	Dr. Kelly E. Fletcher, Performing the Duties of DoD Chief Information Officer of the Department of Defense

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance:

- Establishes policy and assigns responsibilities for support to DoD Information Network (DODIN) operations, which includes the DoD-wide operational, organizational, and technical capabilities for securing, operating, and defending the DODIN.
- Adopts the term "DODIN," to be used throughout DoD instead of the term "Global Information Grid."

TABLE OF CONTENTS

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to:

(1) 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 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").

(2) The DODIN, which comprises the set of information capabilities and associated processes for collecting, processing, storing, disseminating, and managing information on-demand for warfighters, policy makers, and support personnel, whether interconnected or stand-alone. This includes owned and leased communications and computing systems and services, software (including applications), data, security services, other associated services, and national security systems within DoD.

(3) DODIN operations, which encompass operations to secure, configure, operate, extend, maintain, and sustain DoD cyberspace to create and preserve the confidentiality, availability, and integrity of the DODIN.

(4) All DoD information systems (IS); DODIN-connected National Security Systems (NSS) or DODIN-connected systems that support NSS; associated processes, personnel, and technology; and DoD interfaces to mission partners.

(5) DoD-owned and -controlled IS operated by a contractor or other entity on behalf of DoD that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity.

b. The U.S. Coast Guard will adhere to DoD requirements, standards, and policies, and will respond to the direction of the Commander, United States Cyber Command (CDRUSCYBERCOM) for U.S. Coast Guard-operated DODIN systems and networks and for U.S. Coast Guard IS and networks that directly affect the DODIN and DoD mission assurance. This will be done while complying with Department of Homeland Security oversight and compliance requirements for acquisition; Section 3541 et seq. of Title 44, United States Code, also known as the "Federal Information Security Management Act;" and financial audit reporting.

1.2. POLICY.

a. DODIN operations will be instituted and conducted to support DoD missions, functions, and operations in a manner that enables authorized users and their mission partners to access and

share timely and trusted information on the DODIN from any location at any time, to the maximum extent allowed by law and DoD policy.

b. DODIN operations are the responsibility of all DoD Components. In accordance with the Unified Command Plan, the mission is assigned to the CDRUSCYBERCOM, to plan, integrate, and coordinate DoD global cyberspace operations, which includes DODIN operations.

c. DODIN operations will be operationally and technically integrated to ensure simultaneous, decentralized, and effective execution.

d. Risk decisions affecting DODIN operations must be coordinated and include cyberspace operations forces with the affected operational authorities in accordance with Directive-type Memorandum 20-004.

e. DoD IS, DODIN-connected NSS, and DODIN-connected systems supporting NSS will be capable of reporting their system status, including fault, configuration, performance, and security to facilitate DODIN health and mission readiness assessments.

f. Data from DoD IS, DODIN-connected NSS, and DODIN-connected systems supporting NSS, including, but not limited to, fault, configuration, performance and security data, will be shared and exchanged through common interoperable standards in accordance with DoD Instruction (DoDI) 8320.02 and direction from United States Cyber Command (USCYBERCOM).

g. A common set of mission-driven metrics, measurements, and reporting criteria will be used to assess DODIN operating performance and to determine the mission impact of service degradations or outages.

h. Requirements for supporting DODIN operations will be addressed and incorporated in doctrine, organization, training, materiel, leadership and education, personnel, facilities, and policy.

i. All acquisition of DoD IS, DODIN-connected NSS, and DODIN-connected systems supporting NSS, will identify and specify requirements for capabilities to support DODIN operations.

SECTION 2: RESPONSIBILITIES

2.1. DOD CHIEF INFORMATION OFFICE (DOD CIO).

The DoD CIO:

a. Provides strategy, policy, guidance, and oversight for support to DODIN operations, including the standards for USCYBERCOM's day-to-day defense and protection of the DODIN across the DoD Enterprise.

b. Ensures acquisition and sustainment of DODIN operations and defense mission capabilities are coordinated, managed, integrated, and synchronized with the Under Secretary of Defense for Acquisition and Sustainment (USD(A&S)), with the Under Secretary of Defense for Research and Engineering (USD(R&E)), and with CDRUSCYBERCOM, the supported mission commander.

c. Establishes necessary agreements with applicable non-DoD and non-U.S. departments, agencies, organizations, mission partners, allies, and coalition partners to facilitate DODIN operations pursuant to DoDD 5144.02.

d. In coordination with the Under Secretary of Defense for Intelligence and Security (USD(I&S)), provides policy guidance to the Director, National Security Agency regarding support to DODIN operations and implementation of cybersecurity policy as described in DoDIs 8500.01," 8510.01, and 8530.01.

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 2.8., the Director, Defense Information Systems Agency:

a. In coordination with the Director, National Security Agency, provides and maintains the minimum essential set of technical standards, specifications, and interfaces, including naming conventions, required for the development and use of interoperable capabilities in accordance with DoDIs 8500.01 and 8530.01.

b. Serves as the Commander, Joint Force Headquarters DODIN, to command and control, plan, direct, coordinate, integrate, and synchronize DODIN operations subordinate to USCYBERCOM in order to secure, operate, and defend the DODIN in support of DoD Component missions.

c. As Commander, Joint Force Headquarters DODIN, develops the mission-driven metrics, measurements, and reporting criteria used to assess DODIN operating performance and to determine the mission impact of service degradations or outages in coordination with the DoD CIO, the CJCS, the Combatant Commanders, and the Military Service Chiefs.

2.3. USD(A&S).

The USD(A&S):

a. In coordination with the DoD CIO, provides direction and guidance concerning the acquisition and sustainment of DODIN operations capabilities and all systems falling under the established definition of the DODIN.

b. Ensures that acquisition and sustainment policies, procedures, and guidance for all DoD IS, DODIN-connected NSS, and DODIN-connected systems supporting NSS, are consistent with and enable DODIN operations in accordance with this issuance.

2.4. USD(R&E).

The USD(R&E):

a. In coordination with the DoD CIO, provides direction, policies, procedures, and guidance for defense research and engineering, technology development, technology transition, prototyping, experimentation, engineering, and developmental testing activities of all DoD IS, DODIN -connected NSS, and DODIN-connected systems supporting NSS.

b. Ensures that research and engineering policies, procedure, and guidance for all DoD IS, DODIN-connected NSS, and DODIN-connected systems supporting NSS are consistent with and enable DODIN operations in accordance with this issuance.

2.5. USD(I&S).

The USD(I&S):

a. Serves as the DoD focal point to the intelligence community for all support to DODIN operations policy and oversight matters relating to intelligence information sharing and interoperability of DoD intelligence systems and processes in accordance with DoDD 5143.01.

b. Requires the Director, Defense Intelligence Agency, as the manager of the sensitive compartmented information (SCI) component of the DODIN, to interact with the Director of National Intelligence and CDRUSCYBERCOM to facilitate coordination and sharing of DoD SCI network status and situational awareness information.

c. Approves DoD Components that may conduct certain intelligence operations and activities in cyberspace in accordance with DoDIs S-5240.09, O-5240.10, S-5240.17, and S- 5240.23.

2.6. DIRECTOR, DEFENSE INTELLIGENCE AGENCY.

Under the authority, direction, and control of the USD(I&S), and in addition to the responsibilities in Paragraph 2.8., the Director, Defense Intelligence Agency:

a. Coordinates with the Intelligence Community (IC), in accordance with procedures approved by the Secretary of Defense and the Director of National Intelligence or their designees, to harmonize any conflicting DoD and IC policies regarding the DoD SCI network.

b. Facilitates coordination and sharing of DoD SCI network status and situational awareness information with CDRUSCYBERCOM.

2.7. DIRECTOR, OPERATIONAL TEST AND EVALUATION.

The Director, Operational Test and Evaluation:

a. Prescribes policies and procedures to test and evaluate operationally DODIN capabilities that are developed and acquired.

b. Monitors and reviews the operational testing of DODIN operations processes, procedures, and capabilities.

2.8. DOD COMPONENT HEADS.

The DoD Component heads:

a. Execute DODIN operations within DoD Component-operated portions of the DODIN in accordance with the Unified Command Plan and in support of the Combatant Commander responsibilities in Paragraph 2.10.

b. Plan, procure, develop, test, and implement capabilities to secure, operate, and defend their segment of the DODIN that are consistent with DoD policy, strategic guidance, and direction from USCYBERCOM, Joint Force Headquarters DODIN, and appropriate Service Cyber Components, issued under the Directive Authority for Cyberspace Operations.

c. Ensure that forces are organized, trained, equipped, and resourced to implement and execute DODIN operations. Ensure that doctrine, organization, training, materiel, leadership and education, personnel, and facilities and related guidance are consistent with this policy.

d. Ensure that DoD IS data is portable between the DoD Components, IC, and contracted vendors' storage in accordance with DoDI 8320.02, the DoD Computing Cloud Security Requirements Guide, and USCYBERCOM direction.

e. Ensure that DoD IS are capable of real time access and reporting of government owned – contractor operated and contractor owned – contractor operated system status including fault, configuration, performance, and security to facilitate DODIN health and mission readiness assessments.

f. Establish and provide the necessary resources to ensure compliance with service-level agreements and memorandums of agreement among DODIN service providers and customers.

g. Participate in the cyberspace operations community of interest (COI) to share information, promote standards, and resolve DODIN operations issues.

h. Ensure that all DoD contractors and other entities operating DoD-owned IS and DoD-controlled IS on behalf of DoD that receive, process, store, display, or transmit DoD information, regardless of classification or sensitivity, comply with this issuance.

i. Accept reciprocity for USCYBERCOM-certified cyberspace operations forces from other services to operate on all Service and Component networks.

2.9. CJCS.

In addition to the responsibilities in Paragraph 2.8., the CJCS:

a. In coordination with the DoD CIO, provides direction and guidance concerning the integration and development of DODIN operations capabilities in the Joint Capabilities Integration and Development System process, including directing the appropriate changes to achieve target capability increments and ensuring that the Combatant Commands' enterprise architectures address existing and future DODIN operations capability requirements.

b. In coordination with the Combatant Commanders:

(1) Advocates for and supports joint force enterprise architectures to address existing and future DODIN operations capability requirements.

(2) Identifies DODIN operations capabilities needed to support joint, combined, coalition, and other operations with mission partners.

c. Develops, in coordination with CDRUSCYBERCOM, joint DODIN operations policies, guidance, and instructions.

d. Incorporates DODIN operations and planning into joint doctrine.

2.10. COMBATANT COMMANDERS.

In addition to the responsibilities in Paragraph 2.8., the Combatant Commanders:

a. Coordinate DODIN operations to be consistent with functional or geographic responsibilities and USCYBERCOM policies and procedures.

b. Identify DODIN operations requirements to support DoD Components and DoD mission partners.

c. Serve as a focal point for DODIN operations with coalition partners.

d. Retain authority to approve or deny DoD Component-initiated DODIN modifications that impact theater operations.

2.11. CDRUSCYBERCOM.

In addition to the responsibilities in Paragraphs 2.8. and 2.10., the CDRUSCYBERCOM:

a. Directs DODIN operations and defense in accordance with the Unified Command Plan.

b. Identifies DODIN operations characteristics and capabilities in consultation with DoD CIO and the other DoD Component heads.

c. Coordinates intelligence and information-sharing activities involving DoD SCI networks with the IC Security Coordination Center in accordance with the established procedures approved by the Secretary of Defense and the Director of National Intelligence, or their designees, pursuant to memorandums of agreement between the DoD CIO and the IC Chief Information Officer.

d. Advises the CJCS on DODIN operations matters affecting National Military Command System performance, the integrity of the DODIN, or actions needed to support DoD operations as described in DoDI S-5100.92.

e. Coordinates with the DoD CIO and the other DoD Component heads to develop and implement a DODIN operations continuity of operations capability in accordance with DoDD 3020.26.

f. Conducts joint experiments and exercises to develop and refine DODIN operations procedures and requirements.

g. Establishes criteria for classifying DODIN operations information in accordance with Volume 1 of DoD Manual 5200.01.

h. Establishes a DODIN operations COI to provide a forum to share information, promote standards, and resolve DODIN operations issues. The DODIN operations COI will develop and publish a standard set of operations metrics, measurements, and processes to enable consistent enterprise-wide monitoring and assessment of DODIN health, security, and mission readiness.

i. Oversees and synchronizes joint DODIN operations training to ensure commonality and compatibility among the DoD Components.

j. Approves DODIN modifications that have a global impact on theater operations.

2.12. COMMANDER, UNITED STATES SPACE COMMAND.

In addition to the responsibilities in Paragraphs 2.8. and 2.10., the Commander, United States Space Command:

a. Serves as the global satellite communications (SATCOM) operations manager for the SATCOM segment of the DODIN.

b. Allocates limited bandwidth across DoD SATCOM capacity in support of Combatant Command operational requirements.

c. Operates DoD SATCOM satellite assets and defends them from space-based threats.

GLOSSARY

G.1. ACRONYMS.

ACRONYM	MEANING
CDRUSCYBERCOM	Commander, United States Cyber Command
CJCS	Chairman of the Joint Chiefs of Staff
COI	community of interest
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DODIN	DoD Information Network
IC	intelligence community
IS	information systems
NSS	National Security Systems
SATCOM	satellite communication
SCI	sensitive compartmented information
USCYBERCOM	United States Cyber Command
USD(A&S)	Under Secretary of Defense for Acquisition and Sustainment
USD(I&S)	Under Secretary of Defense for Intelligence and Security
USD(R&E)	Under Secretary of Defense for Research and Engineering

G.2. DEFINITIONS.

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

TERM	DEFINITION
cyberspace operations	Defined in Joint Publication 3-12.
DODIN	Defined in Joint Publication 6-0.
DODIN operations	Defined in Joint Publication 3-12.
IS	Defined in Committee on National Security Instruction 4009.

REFERENCES

Committee on National Security Systems Instruction 4009, "Committee on National Security Systems Glossary," April 6, 2015

Directive-type Memorandum 20-004, "Enabling Cyberspace Accountability of DoD Components and Information Systems," November 13, 2020

DoD Computing Cloud Security Requirements Guide, March 6, 2017, as amended

DoD Directive 3020.26, "DoD Continuity Policy," February 14, 2018

DoD Directive 5143.01, "Under Secretary of Defense for Intelligence and Security (USD(I&S))," October 24, 2014, as amended

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

DoD Instruction S-5100.92, "Defense and National Leadership Command Capability (DNLCC) Governance (U)," May 11, 2009[1]

DoD Instruction S-5240.09, "(U) Offensive Counterintelligence Operations (OFCO)," February 2, 2015, as amended[2]

DoD Instruction O-5240.10, "Counterintelligence (CI) in the DoD Components," April 27, 2020

DoD Instruction S-5240.17, "(U) Counterintelligence Collection Activities (CCA)," March 14, 2014, as amended[3]

DoD Instruction S-5240.23, "Counterintelligence (CI) Activities in Cyberspace (U)," December 13, 2010, as amended[4]

DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 3, 2015, as amended

DoD Instruction 8500.01, "Cybersecurity," March 14, 2014, as amended

DoD Instruction 8510.01, "Risk Management Framework (RMF) for DoD Information Technology (IT)," March 12, 2014, as amended

DoD Instruction 8530.01, "Cybersecurity Activities Support to DoD Information Network Operations," March 7, 2016, as amended

DoD Manual 5200.01, Volume 1, "DoD Information Security Program: Overview, Classification, and Declassification," February 24, 2012, as amended

Joint Publication 3-12, "Cyberspace Operations," June 8, 2018

Joint Publication 6-0, "Joint Communications System," June 10, 2015, as amended

Unified Command Plan, current edition[5]

United States Code, Title 44, Section 3541 et seq. (also known as the "Federal Information Security Management Act")

1 Available on the Secret Internet Protocol Router network.

2 Available on the Secret Internet Protocol Router network.

3 Available on the Secret Internet Protocol Router network.

4 Available on the Secret Internet Protocol Router network.

5 Available on the Secret Internet Protocol Router network.