DoD Instruction 8010.01

Department of Defense Information Network (DODIN) Transport

Originating Component:	Office of the Chief Information Officer of the Department of Defense
Effective:	September 10, 2018
Releasability:	Cleared for public release. Available on the Directives Division Website at http://www.esd.whs.mil/DD/.
Approved by:	Essye B. Miller, Acting DoD Chief Information Officer

Purpose: In accordance with the authority in DoD Directive (DoDD) 5144.02, this issuance establishes policy, assigns responsibilities, and provides procedures for DODIN transport and the life-cycle management of:

- Connection and interconnection of information systems (e.g., applications, enclaves, or outsourced processes).
- Unified capabilities (UC) products (including data, voice, and video).
- Access to information services (including data, voice, video, and cross domain (CD)) transmitted over the DODIN transport.

TABLE OF CONTENTS

FIGURES

SECTION 1: GENERAL ISSUANCE INFORMATION

1.1. APPLICABILITY.

a. This issuance applies to 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 DoD (referred to collectively in this issuance as the "DoD Components").

b. The Coast Guard will adhere to DoD cybersecurity requirements, standards, and policies, and will be responsible to the direction of Commander, U.S. Cyber Command, for Coast Guard-operated DoDIN systems and networks and for Coast Guard information systems and networks that directly affect the DoDIN and DoD mission assurance, while complying with DHS oversight and compliance requirements for acquisition, the Federal Information Security Management Act, and financial audit reporting.

1.2. POLICY.

a. DoD Components will use designated DoD-wide architectures, enterprise services, data and technical standards, and interoperability for information technology (IT) and National Security Systems (NSS) approved by the DoD Chief Information Officer (CIO) through the Enterprise Architecture and Services Board to improve network effectiveness, optimize delivery of capabilities, improve interoperability, enhance situational awareness of DODIN transport and interconnected networks, and facilitate faster response to cyber threats.

b. DoD Components will reduce duplication, optimize usage, and improve efficiency in the delivery of DODIN transport services.

c. DoD Components:

(1) Will use DODIN transport solutions to establish reliable and secure network connections with mission partners.

(2) Will have the appropriate level of information confidentiality, integrity, and availability for differing security domains to support mission assurance objectives for DoDIN network connections.

(3) Will use the Defense Information System Network (DISN) as the core element of DODIN transport.

(4) Must implement and register all connections to the DISN, including DoD Component and mission partner systems connected to DISN gateways, in the DODIN tracking and management repository in accordance with the DISN Connection Process Guide (DCPG) and DISN Cloud Connection Process Guide (DCCPG). The DCPG and DCCPG (until integrated

with the DCPG) are available at: http://www.disa.mil/Services/Network-Services/Enterprise-Connections/.

d. DODIN transport infrastructure must be protected using DoD's policies, strategies, and architectures for trusted systems and networks, the risk management framework (RMF), and the DoD cybersecurity processes to eliminate or mitigate vulnerabilities and assure minimum levels of security for collaboration activities throughout DoD, in accordance with DoD Instruction (DoDI) 5200.44, DoDI 8500.01, DoDI 8510.01, DoDI 8523.01, DoDI 8530.01, DoDI 8540.01, and DoDI 8551.01.

e. DoD Components will use the DISN-provided transport, when available, to satisfy DoD information transfer requirements between DoD installations and facilities, and DISN-provided gateways for connections to mission partner networks and information systems.

f. Network management and cybersecurity situational awareness of the DODIN transport and its connections, and interconnections of information systems, UC products, and information services will be instituted and conducted to support DoD missions, functions, and operations. It must enable authorized users and their mission partners to securely access and share timely and trusted information on the DODIN from any location at any time, to the maximum extent allowed by law and DoDI 8410.02 and DoDI 8410.03.

g. Direction of DODIN operations and defense will be in accordance with the Unified Command Plan.

h. Negotiations and conclusion of international agreements related to the sharing or exchange of DoD communications equipment, facilities, support, services, or other communications resources, as identified in Section 2350(f) of Title 10, U.S. Code, must be conducted in accordance with DoDD 5530.3.

SECTION 2: RESPONSIBILITIES

2.1. DOD CIO. The DoD CIO:

a. Monitors, evaluates, and provides advice to the Secretary of Defense regarding all DODIN transport activities, and oversees implementation of this issuance.

b. Develops and establishes DODIN transport policy and guidance, comprised of the DISN and DoD Component enclaves, consistent with this issuance and applicable federal law and regulations.

c. Establishes DODIN technical reference and solutions architectures, standards, technical profiles, and supporting enterprise services to address transport connection requirements.

d. Oversees DoD's risk executive functions and supporting bodies to assess and provide strategic guidance to mitigate risk affecting DODIN transport.

e. Provides oversight and policy for DODIN transport connections and for external facing DODIN, including DISN and DoD Component enclave access points and boundary protections.

f. Reviews and approves the integrated DCPG to provide procedures for managing and ensuring the operational utility and security of connections to the DISN and the process of connecting a mission owner to a cloud service offering (CSO) respectively.

g. Reviews and approves DoD Component requests for mission partner connections to the DISN, and establishes agreements with federal departments and agencies, consistent with guidance in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-47, and coalition partners where applicable.

h. Reviews and provides recommendations to the Secretary of Defense on DODIN budget requests and the management of DODIN information resources. This includes the DODIN transport and its connections and interconnections of information systems; UC products; and information services.

i. Reviews and approves a DODIN Transport Optimization Plan.

2.2. DIRECTOR, DEFENSE INFORMATION SYSTEMS AGENCY (DISA). Under the authority, direction, and control of the DoD CIO and in addition to the responsibilities in Paragraph 2.10, the Director, DISA:

a. Ensures that DISN capabilities and its access points and boundary protections are planned, engineered, procured, operated, maintained, and managed to meet DoD mission requirements and improved effectively and efficiently for end-to-end interoperability through technical refresh, technical evolution, and sustainment, in accordance with DoDD 5105.19.

b. Plans, programs, budgets and executes DISN resources in accordance with DoDD 7045.14.

c. Promotes a standard system for naming and categorizing IT components of and develops DISN technical and solution architectures.

d. Provides CD enterprise services and integrates new CD information transfer requirements into DoD enterprise CD services, in accordance with DoDI 8540.01.

e. Serves as Commander, Joint Force Headquarters DODIN (JFHQ-DODIN), to command and control, plan, direct, coordinate, integrate, and synchronize DODIN operations and defensive cyberspace operations – internal defense measures (DCO-IDM) in order to secure, operate, and defend DODIN transport, in support of DoD, Combatant Command, Military Service, and Defense Agency missions.

f. Plans, engineers, acquires, tests, fields, and supports global communications solutions for the DISN to serve the needs of the President, the Vice President, the Secretary of Defense, and the DoD Components.

g. Directs operation and management and maintains configuration management of the DISN to meet DoD Components operational requirements, including UC as defined in DoDI 8100.04.

h. Identifies, coordinates, and documents requirements to support DISN equipment at locations utilized for DoD missions.

i. Develops and implements technical solutions for the DISN to close joint capability gaps, including the Mission Partner Environment (MPE), received through the Joint Capabilities Integration and Development System process in accordance with CJCS Instruction 3170.01.

j. Prepares to extend the DISN, upon a Combatant Commander's request, to support DoD contingency operations around the world.

k. Publishes a catalog of DISN services with rates that are established in accordance with DoDD 5118.03.

l. Develops, distributes, and maintains an integrated DCPG, updated annually, to describe steps and requirements for connection to the DISN and for mission owners to connect to CSOs.

m. Develops, distributes, maintains, and implements cybersecurity for the DISN in accordance with DoDI 8500.01.

n. Develops and maintains an integrated joint tracking and management repository of DODIN connections (e.g., DISN, commercial, Component, mission partner), that includes technical and operational characteristics, whether physical or virtual, and is accessible by DoD Components.

o. Implements a process to discontinue DISN connections that are inactive for more than 6 months and include consideration for connections used to support continuity of operations in coordination with the responsible organization.

p. Authorizes the Secret Internet Protocol (IP) Router Network (SIPRNet) to process North Atlantic Treaty Organization secret information, in accordance with U.S. Security Authority for North Atlantic Treaty Organization Affairs Instruction 1-07, U.S.-only information, and secret information releasable to Five Eye partners.

q. Conducts onsite and remote SIPRNet, Non-classified Internet Protocol Router Network (NIPRNet), and releasable mission network compliance scanning, cybersecurity-related monitoring, vulnerability assessments, compliance validation, and cybersecurity inspections, as directed by the Commander, U.S. Cyber Command (CDRUSCYBERCOM).

r. Develops and uses performance metrics to assess DODIN transport, its connections, and DISN capabilities in coordination with the DoD CIO, the Under Secretary of Defense for Intelligence (USD(I)), and the CJCS.

s. Reviews, processes, and approves DoD Component-validated DISN connection requests.

t. Provides cybersecurity services, when requested, for mission partner networks (federal department, federal agency, or coalition partners) connected to SIPRNet or via the SIPRNet mission partner gateway (MPGW); identifies non-compliance issues; and recommends remediation to the appropriate organization. At the direction of DoD CIO, assesses whether a mission partner's cybersecurity services are equal to requirements in DoDI 8530.01, and provides a detailed report to the DoD CIO on a reimbursable basis.

u. Establishes funds transfer agreements with federal department and federal agency mission partners in compliance with DoDI 4000.19 and Section 1535 of Title 31, U.S. Code and outlines terms for mission partners to reimburse DoD for costs associated with DISN connections and any reimbursable DISA-provided enterprise services the mission partners request and the DoD CIO approves.

v. Establishes a management system, conducts periodic audits, and ensures selection of the most economical means for satisfying all base and long-haul telecommunications requirements, consistent with applicable law and policy guidance.

w. Develops funding and cost recovery models, policies, and procedures, and publishes rates for all DISN capabilities, including computing and MPE (federal department, federal agency, and coalition partner) connections to DISN in coordination with DoD Components and in accordance with DoDD 5118.03.

x. Develops and maintains an annual DODIN Transport Optimization Plan.

y. Serves as the lead integrator for DODIN transport capabilities (e.g., DISN, airborne, intelligence, surveillance, and reconnaissance data transport) with support that includes, but is not limited to, systems engineering for end-to-end interoperability, system performance criteria, integrated architectures, standards, profiles, and spectrum management.

2.3. UNDER SECRETARY OF DEFENSE FOR POLICY (USD(P)). The USD(P) provides coordination and support for mission partner connections to the DODIN transport, including international agreements as specified in DoDD 5530.3 and Department of Homeland Security agreements as specified in DoDI 3025.19.

2.4. UNDER SECRETARY OF DEFENSE FOR RESEARCH AND ENGINEERING. The Under Secretary of Defense for Research and Engineering establishes policies on, and supervises, all defense research and engineering, technology development, technology transition, prototyping, experimentation, and development testing activities and programs, including the allocation of resources and unifying these efforts across the Department, in accordance with Deputy Secretary of Defense Memorandum, that support the policy in this issuance.

2.5. UNDER SECRETARY OF DEFENSE FOR ACQUISITION AND SUSTAINMENT. The Under Secretary of Defense for Acquisition and Sustainment establishes policies on and supervises all elements of the Department relating to acquisition and sustainment and policies on contract administration, in accordance with Deputy Secretary of Defense Memorandum, that support the policy in this issuance.

2.6. USD(I). The USD(I) oversees the Director, Defense Security Service (DSS), to maintain a complete program of authorization and oversight of defense contractor information systems used to process and store classified information at cleared defense contractor facilities pursuant to DoDI 5220.22 and DoD 5220.22-M.

2.7. DIRECTOR, DEFENSE INTELLIGENCE AGENCY (DIA). Under the authority, direction, and control of the USD(I) and in addition to responsibilities in Paragraph 2.10, the Director, DIA:

a. Implements, operates, manages, and defends Joint Worldwide Intelligence Communications System (JWICS) components and facilities on DISN in accordance with established agreements with DISA.

b. Establishes connections to JWICS in accordance with DIA Instruction 8550.002.

c. Provides threat assessments to support DoD Components systems and system risk assessments and decisions.

2.8. DIRECTOR, NATIONAL SECURITY AGENCY/CHIEF, CENTRAL SECURITY SERVICE. Under the authority, direction, and control of the USD(I) and in addition to responsibilities in Paragraph 2.10, the Director, National Security Agency/Chief, Central Security Service:

a. Recommends techniques and procedures to minimize DODIN transport cybersecurity vulnerabilities in accordance with DoDI 8500.01.

b. Develops and certifies DODIN transport communications security (COMSEC) solutions and produces keying material for COMSEC in accordance with DoDI 8523.01.

2.9. DIRECTOR, DSS. Under the authority, direction, and control of the USD(I) and in addition to responsibilities in Paragraph 2.10, the Director, DSS:

a. Establishes security standards as the authorizing official (AO) for defense contractor classified systems in accordance with DoD 5220.22-M.

b. Requires defense contractor classified systems connected to the DODIN transport to be in compliance with contract security provisions in accordance with DoDI 5220.22, DoD 5220.22-M, and DSS developed guidance.

c. Notifies DoD Component sponsors about non-compliant defense contractor connections to SIPRNet.

d. Requires defense contractor systems that process classified information connected to DODIN transport be aligned to a DoD network operations and security center and supporting cybersecurity services provider in accordance with DoDI 8530.01.

e. Maintains a memorandum of agreement (MOA) outlining roles and responsibilities for both DISA and DSS in the connection approval process and oversight of cleared defense contractor connections to DODIN transport through the DISN.

f. Establishes cybersecurity inspection teams that include team members from DISA or USCYBERCOM, as appropriate, to conduct DSS compliance inspections and support USCYBERCOM-directed command cyber readiness inspections (CCRIs) of defense contractor classified systems connected to DODIN transport in accordance with DoDI 5220.22, DoD 5220.22-M, and contract system security provisions.

g. Provides cybersecurity inspection results upon request to CDRUSCYBERCOM, DoD CIO, and Director, DISA for defense contractor systems processing classified information connected to DODIN transport.

2.10. UNDER SECRETARY OF DEFENSE (COMPTROLLER)/CHIEF FINANCIAL OFFICER, DEPARTMENT OF DEFENSE (USD(C)/CFO). The USD(C)/CFO advises the Secretary of Defense on budgetary and financial matters for DODIN transport and collaboratively develops, reviews, and recommends funding and cost recovery policies and procedures through the Defense Working Capital Fund Corporate Board in accordance with DoDD 5118.03.

2.11. DOD COMPONENT HEADS. The DoD Component heads:

a. Plan, program, budget, and execute resources to support the DISN and other DODIN transport as required.

b. Procure, operate, manage, and maintain their portion of DODIN transport and the supporting infrastructure in accordance with this issuance.

c. Comply with applicable cybersecurity issuances, Security Technical Implementation Guides, security requirements guides, and other guidance developed and distributed by appropriate authorities.

d. Monitor cyber activities, initiate appropriate action in response to cybersecurity incidents, and implement orders and directives related to DODIN transport and connected systems and networks, issued by CDRUSCYBERCOM, and JFHQ-DODIN including:

(1) Mitigations and remediation in response to vulnerabilities and threats to DODIN and connected systems and networks.

(2) Disconnection of systems or networks to DODIN transport when a threat or vulnerability poses a risk to the DODIN, a connection is no longer needed, the connection does not have a current authority to operate.

(3) Notification to DSS of those cybersecurity incidents involving cleared defense contractors that occur on the DODIN and the related subsequent developments and resolution of the incidents.

e. Establish support agreements (e.g., contracts, MOAs) with their mission partners (e.g., sponsored defense contractors, and federal and foreign entities) that stipulate conditions and responsibilities to jointly implement, operate, manage, and protect authorized circuit interconnection with DODIN transport.

f. Use an enterprise CD service or centralized cross-domain solution for automated DoD CD information transfer requirements but limit proliferation and ensure secure implementation in accordance with DoDI 8540.01.

g. Collaborate with DISA regarding identified and validated joint capability gaps to facilitate efficient and synchronized development of enterprise solutions.

h. Establish an MOA with DISA to document site support terms and responsibilities for DISN equipment located on DoD Component installations or facilities, in accordance with DoDI 4000.19, and a site concurrence letter(s) as an appendix to an MOA to document individual project requirements, in accordance with DISA Circular 310-55-9.

i. Ensure that a host tenant support agreement (HTSA) is established between DoD Component installation hosts and tenant organizations to provide material and services to support connection of authorized tenant organization systems and users, in accordance with DoDI 4000.19.

j. Ensure that requirements for connections to the DISN, including DoD Component enclave connections, are approved, documented, and submitted in accordance with the DCPG and DCCPG (until integrated with the DCPG). Establish an approval process for DODIN transport not specifically addressed.

k. Maintain situational awareness of the cyberspace environment affecting systems, DODIN infrastructure, and any inherent external connections to the DISN, mission partners, or an internet service provider.

l. Ensure that all DoD Component systems and networks connected to DODIN transport comply with the DoD cybersecurity program, in accordance with DoDI 8500.01, and certification for interoperability, in accordance with DoDI 8330.01, and adequately tested, in accordance with DoDI 5000.02.

m. Require systems connected to DODIN transport to have an authorization to operate (ATO) and implement the RMF in accordance with DoDI 8510.01.

n. Ensure that DoD Component systems integrate and employ cybersecurity activities to support DODIN operations and DCO-IDM in accordance with DoDI 8530.01.

o. Require mission partner systems connected to DODIN transport have an ATO, in accordance with applicable DoD, Committee on National Security Systems, Intelligence Community (IC), NIST, or equivalent cybersecurity policies and processes, as stipulated in support agreements, MPE joining, membership, and exit instructions, or contracts.

p. Develop and maintain an annual DoD Component Annex to the DODIN Transport Optimization Plan, including data transport cycle upgrades and new transport capabilities.

q. Conduct reviews of a subset of implemented systems security controls for compliance at least annually and continuously monitor the security status of systems in accordance with DoDI 8500.01, DoDI 8510.01, and supplemental DoD Component guidance.

r. Inform Combatant Commanders of connection requirements impacting operational missions within their respective areas of responsibility.

s. Implement DODIN transport commercial wireless devices, services, and technologies using applicable cybersecurity guidance in accordance with DoDD 8100.02, DoDI 8420.01, and DoDI 8500.01.

t. Ensure management of local interfaces between DoD Component voice networks, the Defense Switched Network, and access to Commercial Voice over IP (VoIP) telecommunications services and the Public Switched Telephone Network via controlled Commercial VoIP network access points to the internet telephony service provider. Ensure that DISN and commercial connections interface through a peering arrangement via a DoD CIO-approved gateway designed to minimize risk to the DODIN.

u. Identify connection compliance issues and recommend mitigation and remediation actions to the appropriate risk executive management authorities in accordance with DoDI 8500.01 and DoDI 8510.01.

v. Discontinue services that are no longer needed or are not economical where mission continuation is not justified.

w. Publish guidance on authorized and prohibited uses of DODIN transport in accordance with DoDD 5500.07.

x. Ensure interoperability of equipment connected to the DISN in accordance with DoDI 8330.01.

y. Ensure that all DoD Component and mission partner systems and network connections that travel the DISN/DODIN transport are registered in the DoD Ports, Protocols, and Services Management Registry in accordance with DoDI 8551.01.

z. Ensure conformance with IT service management standards in accordance with DoDI 8440.01.

aa. Direct MINIMIZE for all, or part of the DoD Component enclave, including staffs and subordinate organizations based on operational needs.

(1) Provide subordinate organizations guidance on the preparation and procedures to implement MINIMIZE to:

(a) Maintain communications for command and control on all networks.

(b) Shut down lower priority services to conserve limited bandwidth for critical communications.

(2) Inform the CJCS, CDRUSCYBERCOM, and other DoD Components when MINIMIZE is imposed, modified, or canceled and indicate the type of voice, video, and data communications traffic to be reduced and/or removed.

(3) Ensure compliance with MINIMIZE procedures.

ab. Leverage commercial IP network transport and cloud services available on Defense IT Contracting Organization contracts to connect securely to the DISN services if DISN service is not available at the required operating location.

ac. Direct use of the DISA Direct Storefront (https://disa-storefront.disa.mil/dsf/sfoverview) to obtain DODIN transport services (including all commercial connections). Ensure that all DODIN transport connections are updated in DISA's integrated joint tracking and management repository for physical and virtual connectivity.

ad. Use existing federal or DoD enterprise contracting vehicles for services that meet the DoD Component's mission requirements.

ae. Ensure wireless equipment complies with existing domestic, regional, and international frequency spectrum allocations and regulations (e.g., National Telecommunications & Information Administration Manual of Regulations and Procedures for Federal Radio Frequency Management).

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

a. Develops, coordinates, and establishes a process to collect, validate, prioritize, and sustain operational requirements for the MPE and its connections to DODIN, in accordance with DoDI 8110.01.

b. Supports Combatant Command requests for mission partners, including defense contractors and connections to DODIN transport in support of joint missions and operations.

c. Provides support for the development of international agreements for the connection of foreign mission partners to DODIN transport, as specified in DoDI 4000.19 and DoDD 5530.3, in coordination with USD(P).

d. Develops operational procedures for implementing MINIMIZE controls on users or voice, video, and data communications including, but not limited to, blocking, routing, usage, or availability controls.

2.13. CDRUSCYBERCOM. In addition to responsibilities in Paragraph 2.10, the CDRUSCYBERCOM:

a. Directs the security, operations, and defense of the DODIN, in accordance with Unified Command Plan and DoDI 8530.01.

b. Issues orders and directives to all DoD Components for the execution of Global DODIN operations and DCO-IDM to compel unity of action to secure, operate, and defend the DODIN in accordance with directive authority for cyberspace operations, delegable to Commander, JFHQ-DODIN.

c. Directs CCRIs of DODIN transport and connected systems, in accordance with DoDI 8500.01.

d. Issues procedures for conducting remote compliance monitoring and scanning of systems connected to DODIN transport.

e. Directs MINIMIZE for all or part of the DODIN based on operational needs, indicates the type of voice, video, and data communications traffic to be reduced or removed, and informs CJCS when MINIMIZE is imposed, modified, or canceled within the DODIN.

f. Under the authority of the January 19, 2017 Memorandum of Agreement between the Departments of Defense and Homeland Security:

(1) For purposes of securing, operating, and defending the DoDIN, the CDRUSCYBERCOM:

(a) Directs and receives reports from the Coast Guard Cyber Command.

(b) Defends Coast Guard-operated DoDIN systems and networks as part of its overarching defense of the DoDIN.

(2) CDRUSCYBERCOM is permitted to operate on Coast Guard-operated information systems and networks that directly affect the DoDIN and DoD mission assurance for the purposes of securing, operating, and defending the DoDIN.

(3) CDRUSCYBERCOM is authorized, under applicable legal authorities (e.g., Section 1535 of Title 31 ("the Economy Act") and Chapter 15 of Title 10, U.S. Code), to approve support, on a reimbursable basis, to the Coast Guard for its non-DoDIN systems and networks.

(a) This authority does not include support to law enforcement investigations or activities, which is governed in accordance with DoD Instruction 3025.21.

(b) CDRUSCYBERCOM will notify the CJCS and the Under Secretary of Policy, through the Assistant Secretary of Defense for Homeland Defense and Global Security, upon approval of such support.

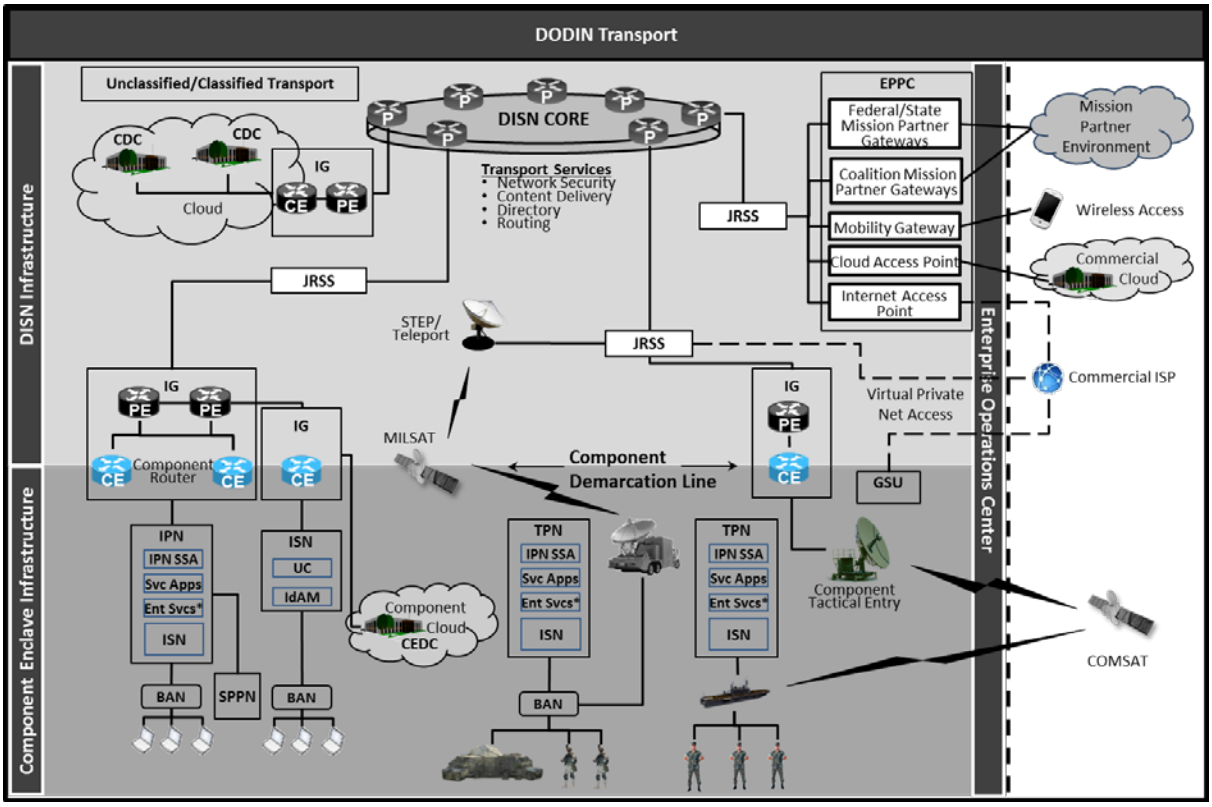
SECTION 3: DODIN TRANSPORT

3.1. DODIN TRANSPORT. The DODIN (i.e., transport) and the associated network services contain various dissemination elements required to operate, maintain, and secure required distribution capabilities.

a. The DODIN consists of all networks and information systems owned or leased by DOD. The DODIN includes common enterprise service networks (classified and unclassified), intelligence networks operated by DoD Components within the IC, closed mission system and battlefield networks, and other special purpose networks.

b. The DISN and DoD Component enclaves provide the two main network transport elements of the DODIN as shown in Figure 1 with the demarcation points delineated.

Figure 1. DODIN Transport



c. All DODIN transport reference and solution architectures follow the DoD Enterprise Architecture and Joint Information Environment (JIE) Enterprise Reference and Solution Architectures (e.g., Satellite Communications (SATCOM) Gateway Solution Architecture, wide area network Solution Architecture), available at https://wmaafip.csd.disa.mil/Home (NIPRNet) and https://wmaafip.csd.disa.smil.mil/Home (SIPRNet). New architectures require approval from the Enterprise Architecture and Services Board.

d. The Combatant Command and subordinate Military Service components have primary responsibility for the deployed warfighter and associated infrastructure within the theater.

3.2. DISN. The DISN provides DoD's worldwide enterprise-level telecommunications and computing infrastructure as the core capability for end-to-end information transfer to support military operations as part of the JIE and is under the operational direction and management control of DISA.

a. The DISN is designated as a mission critical National Security System and must be operated in accordance with DISA Circular 310-130-2.

b. DISN transport provides connectivity for all classification levels among DoD sustaining bases (e.g., bases, camps, posts, and stations); deployed forces; authorized mission partners; and other U.S. Government agencies for the purpose of conducting DoD business. It also provides connectivity to global internet resources and commercial mobile networks. It is designed to be transparent to the joint force.

c. The DISN facilitates management of information resources and is responsive to national security as well as DoD needs. It provides integrated network, cybersecurity, telecommunication, and application services and capabilities (e.g., voice, video, teleconferencing, imagery, satellite, and data services) to DoD sustaining bases, deployed forces, and authorized mission partner locations.

d. The DISN supports the following classification levels and associated connectivity requirements:

(1) Unclassified transport, through DISA's NIPRNet service, provides:

(a) DoD customers with centralized and protected access to the public internet.

(b) Data, voice, and video telecommunication and application services for combat support and business applications to DoD.

(c) Access to the internet through controlled internet access points (IAPs).

(d) Access to commercial cloud service provider's (CSP) CSO through a controlled cloud access point (CAP).

(e) Access to commercial VoIP telecommunications services and the Public Switched Telecommunications Network via controlled commercial VoIP network access points to the internet telephony service provider.

(2) Classified transport, through DISA's SIPRNet service, provides:

(a) Connectivity to mission partner networks.

(b) IP-based secret information transfer throughout DoD for official DoD business applications.

(c) IP-based secret releasable information transfer for U.S. and mission partner information-sharing enclaves on multinational enclaves through MPGWs.

(d) DoD customers with centralized and protected connectivity to federal, IC, defense contractor, and allied information at the secret level.

(e) Support for secret voice and video telecommunication services and UC applications for combat and business communication support to DoD.

(3) Classified transport for JWICS, through the DISA Top Secret/Sensitive Compartmented Information IP Data Service, provides a secure high-speed multimedia communication service between Top Secret/Sensitive Compartmented Information users. It is designed to support the DoD Intelligence Information System community through the DIA Regional Support Center and supports DoD's efficiency initiatives through the use of an IP-based infrastructure. This ensures appropriate security, performance, reliability, and resource management.

(4) Secret releasable and below mission network transport (Common Mission Network Transport) provides virtual private network (VPN) connectivity within the MPE construct. VPN connectivity is neither on nor tunneled through the SIPRNet. Common Mission Network Transport provides IP-based secret releasable information transfer for U.S. and mission partner information sharing enclaves for allied, coalition, interagency, and bilateral Community of Interest networks.

e. The following are not considered part of the DISN, but must follow DISA specifications for the interconnection and interface standards when connected to DISN networks:

(1) Mobile or transportable communications facilities and assets organic to the Military Departments unless specifically designated as components of the DISN.

(2) Platform-specific and other tactical telecommunications.

(3) Installation user or subscriber facilities and terminals.

(4) On-site telecommunications facilities associated with, or integral to, weapons systems and missile launch complexes.

(5) On-site telecommunications infrastructures and facilities at an installation, except where designated as part of the DISN in formal agreements.

(6) Consoles and display devices integral to the command centers of the Combatant Commands, their DoD Component headquarters, and the Military Services' operations centers.

f. The DISN also provides a common set of transport services to support network security, addressing, and content delivery requirements. The MPGW, IAP, CAP, and Mobility Gateway

(MGW)), known collectively as the "Enterprise Perimeter Protection Capability," along with SATCOM gateways, deliver the first line of protection for the DODIN by providing a secure connection between DoD, mission partner and commercial users, networks and systems, and the DISN. Other services include Joint Regional Security Stacks (JRSS), Global Content Delivery Service, Enterprise Directory Service, and Enterprise CD Services. Below are key aspects for some of these capabilities:

(1) JRSS enables network boundary protection and uniform cybersecurity capabilities across all DoD Component networks by providing enterprise-level views of the DODIN with a standardized security topology; applies advanced threat analysis against DODIN network transactions; and improves enterprise responsiveness in assessing, detecting, and responding to threats.

(2) Internet traffic will flow through one of the authorized IAPs, unless the DoD CIO has authorized alternate connectivity (e.g., intelligence, law enforcement, or other specific mission requirements).

(3) SATCOM gateways provide secure and interoperable global access to DISN services via fixed satellite equipment and systems. They possess organic equipment to provide centralized integration capabilities, contingency capacity, and common interfaces so that forward-deployed users may access various DISN services. DISA manages SATCOM gateways via the SATCOM Configuration Control Board.

(4) MGWs provide and manage the connectivity of the mobile device into the DoD network environment for access to enterprise services.

(a) MGWs encrypt end-user traffic via a mobile VPN and provide for secure dedicated access to DISN voice, video, and data services as well as providing a proxy and traffic filter before it connects to the DISN.

(b) Separate gateways will be established for classified and unclassified access. Where feasible and allowed by security policy, some network infrastructure will be shared to save costs.

g. DISN enterprise services that traverse DISN transport services include voice, video, and data as well as ancillary enterprise and JIE services (e.g., directories, DODIN network security, UC, and content delivery).

3.3. DISN AND DOD COMPONENT ENCLAVE DEMARCATION POINTS.

a. The DISN begins and ends at the equipment under the operational direction and management control of DISA at the physical point at which DISN network equipment ends (network termination interface) and the DoD Component enclave infrastructure begins. This is the demarcation of responsibility between DISA and the Components and occurs in the installation gateway (IG), as depicted in Figure 1.

b. DISA is responsible for operation and maintenance of all DISN core equipment, including Provider Edge (PE) routers, connections from the PE routers to the DISN, and the activities on the primary customer edge (CE) router(s) for an installation, where agreed upon by the DoD Component. DISA will ensure delivery of Joint Multi-Protocol Layer Switching (MPLS)/Joint Regional Security Stack (JRSS) connectivity and DISN services to DoD Components. A DoD Component may request for DISA to provide CE router services. The request will codify operational and resource management responsibilities in an agreement (e.g. MOA), including annual maintenance costs and long term life cycle replacement funding.

c. The installation host (i.e., lead DoD Component on a DoD installation), where no agreement is in place between components of DoD, is responsible for maintaining and operating the physical infrastructure in the IG, including the primary CE router(s) for the installation, any cabling, transmission devices, communication racks, main distribution frames and associated physical space, security, utilities and environmental support required to connect local customers to DISN services. The installation host, in coordination with DISA and the installation tenants, will document operational and resource management responsibilities for the CE routers in a HTSA to ensure Joint MPLS connectivity and DISN services for all installation tenants.

d. Addressing, routing, and equipment supporting tenant-specific systems, networks, and services are the responsibility of the tenant or their designated service provider.

3.4. DOD COMPONENT ENCLAVES.

a. DoD Component enclaves, as part of the DODIN and comprised of telecommunications infrastructure and local common services, support the movement of information between fixed installation and locally deployed networks and services, while also extending access to the DISN and other networks and information systems.

(1) A DoD Component enclave provides information transfer and joint services to all authorized users, networks, and systems at a DoD location under the authority of a DoD Component head. The DoD Component head will determine the scope of the enclave by defining a physical area (DoD installation, leased facility, ship, etc.) or an area of operations (e.g., forward-deployed tactical operations).

(2) A DoD Component enclave is owned, managed, and operated by a DoD Component representative assigned as the host for that installation location. The host is responsible for data transmission within the installation, such as: routing DoD information between local activities, interfacing with DISN infrastructure components, and providing operation and maintenance of the installation's telecommunication infrastructure.

(3) IT information entering or exiting the DoD Component enclaves travels through appropriate cybersecurity protections and an IG to either an installation processing node (IPN), installation service node (ISN), or tactical communication node (TCN) to deliver information services by using DODIN transport capabilities.

(4) Geographically separated units connect to the DISN or DODIN telecommunications transport services using an approved DODIN circuit and IP routing in accordance with this issuance.

b. A DoD Component enclave is composed of physical infrastructure that provides a common transport backbone, which supports access to core DODIN services (e.g., DISN, internet access, and core data centers (CDCs)), local information services (industrial and business control system services, etc.), and connectivity for tenant networks and systems.

(1) Any authorized traffic may traverse the DoD Component enclave within the constraints of applicable federal and DoD policies.

(2) A DoD Component enclave provides common voice, video, and data services for all authorized tenants through agreements established in accordance with DoDD 2010.9, DoDI 4000.19, and DoDI 6055.17 through the IG to an IPN or ISN. Common services include:

(a) Dial tone.

(b) Data hosting for local services that cannot be operationally, technically, or economically serviced from a CDC or CEDC.

(c) Common IT systems to operate and maintain facilities (monitoring, alarming, etc.).

(d) Physical security for infrastructure and those common services.

c. DoD Component enclave components include the IG, IPN, ISN, TCN, area distribution node (ADN), telecommunication room (TR), outside plant duct-bank systems, and premise wiring. These elements deliver telecommunication services aboard DoD installations. The host for a DoD installation is responsible for operating and managing these elements at that location including joint bases and joint regions.

d. The IG connects the DISN through a DoD Component CE router to the internal base area network (BAN), comprised of infrastructure that allows connection of multiple wires, cables, fiber-optic cabling, inner router, modems, channel banks, or any other type of telecommunication transport device at a given installation. This physical interface, which may contain a DISA PE router, provides a separation of responsibilities between DISN provided services and the DoD Component enclave.

e. No connections or access to external services will be demarked in a TR to prevent backside connections into the DISN. Demarcation of all external, off-installation services is either in the IG or the ISN. TRs will be built in accordance with Unified Facilities Criteria 3-580-01 and applicable Occupational Safety and Health Administration standards.

f. Outside plant and premise wiring cabling is integral to connecting DoD Component enclave elements together.

(1) The installation host must ensure that physical connections for networks and systems are made in accordance with the ATO for that system or network.

(2) Information systems and networks that are using DoD-owned cable and do not possess an ATO (e.g., commercial establishments) will be physically separated from information systems and networks possessing ATOs and considered non-ATO connections.

g. Other DoD Component enclave capabilities that provide telecommunication transport services but are not integral to the effective operation of the BAN/LAN are:

(1) SATCOM terminals are permanently affixed assets and equipment located on DoD installations to support specific, enduring missions assigned to a Military Service (e.g., Mystic Star) or TCNs supporting deployed networks. SATCOM terminals supporting specialized missions will not be used for general IT transport requirements that can be met by the DISN.

(2) Radio frequency equipment used for local communications and public safety and force protection missions, including high frequency, very high frequency, extremely high frequency, super high frequency, etc. These assets will not connect directly to the DISN if they are using media or analog gateways that connect to commercial telecommunications infrastructure or services.

(3) Wireless technologies such as world-wide interoperability for Microwave Access, WiFi, and mobile WiFi are capabilities that extend telecommunications access wirelessly. Access to the DISN will be through an approved IAP, CAP, or MGW.

(a) Wireless communications will be limited to within the installation's boundaries, except where authorized for inter-installation connectivity.

(b) Wireless devices used to transmit and receive DoD information will be protected in accordance with DoD cybersecurity policies and guidance and NIST SP 800-97 guidance to help organizations set up wireless networks.

SECTION 4: DODIN TRANSPORT MANAGEMENT

4.1. DODIN OPERATIONS MANAGEMENT.

a. USCYBERCOM, or as delegated to JFHQ-DODIN:

(1) Conducts situational monitoring of the DODIN for DoD Components' mission essential tasks to exercise command and control to mitigate any adverse impact of an event or to mitigate and counter a threat through DODIN operations and DCO-IDM.

(2) Conducts joint planning in support of DoD Components when USCYBERCOM is a supporting command.

(3) Identifies, synchronizes, and de-conflicts competing global and regional DODIN operations priorities.

(4) Directs, verifies, and reports on the defensive posture of the DODIN.

(5) Directs actions by DoD Components to:

(a) Improve the overall readiness posture continuously against an evolving threat.

(b) Establish and maintain an appropriate level of readiness across the DODIN.

(c) Aggregate and disseminate actionable intelligence from threats to the DODIN to proactively inform and drive DODIN operations.

(6) Takes appropriate action up to and including isolation, disconnection, or shutdown of systems (including DoD websites) that are posing a threat or potential threat to operations and security of the DODIN.

b. DoD Component heads:

(1) Manage the configuration, security, operations, maintenance, and sustainment of their respective DoD Component enclaves. Joint bases or joint regions will establish agreements in accordance with DoDI 4000.19 and consolidate operation and management functions of multiple tenant DoD Component enclave capabilities to the host for that location.

(2) Identify a node site coordinator at each B/P/C/S that has an IG to provide onsite coordination and support for DISN equipment located locally.

(3) Provide power, physical security, and floor space for DISN equipment in accordance with an established MOA and annex site concurrence letters.

(4) Implement trouble-ticket software to manage telecommunications infrastructure and equipment that is interoperable with trouble ticket software used to manage switches and routers.

(5) Establish and maintain an inventory database of telecommunications services (e.g., circuits, connections, carrier ethernet private IP or MPLS services) and conduct an inventory, at a minimum, every 2 years.

(6) Establish a review and revalidation program for telecommunications transport equipment and services.

(7) Promptly reconcile all billing for telecommunications services, inventories, and acquisition documents before authorizing payment to ensure that DoD only pays for services received.

(8) Establish and provide the necessary resources to ensure compliance with service-level agreements and MOAs among DODIN service providers and customers.

(9) Ensure that all mission partner entities, including DoD contractors, comply with formal agreements (e.g., contracts, MOAs) to execute configuration, security, operations, maintenance, and sustainment functions when operating DoD-owned or DoD-controlled systems.

(10) Perform interconnections on telecommunications infrastructure to prevent backside or unauthorized cross connections by ensuring that all telecommunication connections, commercial and DISN, terminate appropriately at the IG, IPN, or ISN.

(11) Will not physically connect any platform or information system to the DoD Component enclave without a current ATO.

(a) Any IS that receives, processes, stores, displays, or transmits DoD information must have an ATO before connection in accordance with DoDI 8500.01.

(b) Physical connections will be inventoried no less than bi-annually to ensure that all connected ISs, including platform IT systems, have a current ATO.

(c) Connections for commercial entities (e.g., food establishments, lodging, banks, retailers, DoD contractors) that reside on DoD-owned telecommunications infrastructure will be documented and inventoried. DoD Components physically separate these circuits from DoD information whenever possible.

(12) Ensure that an ATO is obtained before connection of any telecommunications connections or services provided by U.S. Government federal agencies on DoD installations.

(13) Document and make available for inspection all connections to DoD Component enclaves during a CCRI.

4.2. DODIN IT ASSET MANAGEMENT. IT asset management provides an avenue to categorize and maintain positive control of equipment and assets and ensure that DoD-owned equipment is recorded and controlled in accordance with DoDI 5000.64. Cataloging infrastructure equipment utilized on DODIN transport enables the tracking of IT efficiencies and ensures compliance with DoD cybersecurity policies. DoD Components will:

a. Identify and record all non-deployable plant property and equipment or garrison assets that are not considered to be a part of the installation's infrastructure (e.g., real property) in an authoritative property database (e.g. Defense Property Accountability System). This database must have a field to input a serial number, model number, quantity, and nomenclature for each piece of equipment.

b. Conduct physical inventories of all telecommunications equipment at least every 2 years to physically verify equipment has not been exchanged for other non-conforming assets and provide updates to the appropriate database manager. Accountability of assets may be performed via an automatic, real-time, software application in between physical inventories.

c. Document an installation's real property inventory (e.g., cabling, ductbank) for accountability purposes (e.g. Internet Naval Facilities Assets Database Store).

4.3. DODIN TRANSPORT SECURITY MANAGEMENT. Every organization within DoD is responsible for security of DODIN transport and its connections between DoD Component enclaves and non-DoD networks and systems. DoD Components will:

a. Ensure that DoD systems physically and virtually connected to the DODIN are aligned to a network operations security center and supporting cybersecurity service provider(s) in accordance with DoDI 8530.01 before connection.

b. Ensure that DODIN transport service or DISN connection requests for a mission partner system, including defense contract systems, to the DISN-provided transport and information services are sponsored (using a signed agreement (e.g., MOA or contract)), endorsed, validated, and submitted in accordance with DoDI 8500.01, DoDI 8510.01, DoDI 8530.01, and other DoD and Committee on National Security Systems cybersecurity policies, before connection to the DISN.

c. Share DODIN situational awareness data with USCYBERCOM and other DoD Components in accordance with DoDI 8320.02, DoDI 8320.07, DoDI 8410.02, and DoDI 8410.03.

d. Implement situation awareness capabilities to manage network elements that collect and report operational configurations, current operational state, current usage state, available network capacity, and percent of capacity currently committed.

e. Monitor and maintain positive control of DoD-owned telecommunications infrastructure and IT equipment in accordance with DoD 5200.08-R. Only authorized personnel will be allowed unescorted access to enter spaces containing DODIN assets. Unauthorized personnel who need to access these spaces must be escorted by authorized personnel. Signs will be posted in facilities that host DISN and DoD Component infrastructure notifying personnel that the space is a controlled area.

f. Implement the RMF for DoD IT in accordance with DoDI 8500.01 and DoDI 8510.01 for their portions of the DODIN.

4.4. DODIN COMMERCIAL CONNECTIONS. Commercial connections must meet the parameters stipulated in Paragraphs 4.4.a. through i. and additional conditions that the DoD CIO or USCYBERCOM may issue based on identified threats or vulnerabilities.

a. Commercial transport services procured as an alternative to the DISN-provided transport requires compliance with this issuance or DoD CIO review and approval. Commercial connections will only be authorized for unique mission requirements that cannot be met by the DISN and documented within the RMF package.

b. DISA, DoD-wide, and General Services Administration contract vehicles are the authorized vehicles for procuring commercial connections and must be registered in accordance with the DCPG.

c. Authorized commercial connections are subject to CCRIs to ensure conformance with DoD cybersecurity requirements consistent with DoDI 8510.01, DoDI 8530.01, and other DoD cybersecurity policies and guidance.

d. DISN special service offerings that support a government mission, use government-owned equipment, and do not adversely affect the mission need are available at https://www.disa.mil/Network-Services/VPN.

e. DoD Components will ensure that commercial connections adhere to specific conditions in accordance with the DCPG including but not limited to:

(1) The sensitivity of the data being processed, stored, and transmitted.

(2) Processes for non-DODIN access.

(3) An annual review for need and compliance.

(4) Protected information.

(5) Equipment used by the DoD Component on the DoD Approved Products List (https://aplits.disa.mil/apl/).

(6) Physical or logical separation.

(7) Transitioning to DISN.

(8) Best cost and benefit solution (Template at https://dodcio.defense.gov/Portals/0/Documents/DOD%20IT%20Business%20Case%20Analysis%20(BCA).pdf)

(9) The 10-year procurement time limit, in accordance with DoDI 7000.14-R.

f. The following types of unclassified commercial connections may be used to transmit Controlled Unclassified Information, as described in the DCPG:

(1) Connections to temporary facilities.

(2) Infrastructure non-availability.

(3) Urgent and ad hoc mission (up to 90 days).

(4) Temporary training (less than 90 days).

(5) Non-DoD locations.

g. The following types of unclassified commercial connections that support unique information systems and missions require appropriate DoD cybersecurity controls applied by the DoD Component AO, as described in the DCPG:

(1) Enduring training and education.

(2) Missions requiring non-attribution.

(3) Support to civil-military operations, in accordance with DoDI 8220.02, DoDI 3000.05, and DoDI 3003.01.

h. The following types of unclassified commercial connection requirements may be used to transmit data, as described in the DCPG:

(1) Force protection and public safety in accordance with DoDDs 3020.44, 3025.13, and 3025.18 and DoDIs 5535.10 and 6055.17.

(2) Civil authority database in accordance with Directive-type Memorandum 09-012.

(3) Payment card in accordance with DoDD 5400.11.

i. The AO will tailor appropriate security controls for the following non-DISN requirements that process, store, and transmit publically releasable DoD data, as described in the DCPG:

(1) Community relations events in accordance with DoDI 5410.19.

(2) Non-appropriated fund instrumentalities in accordance with DoD 7000.14-R and DoDIs 1015.10 and 1015.15.

(3) Morale, welfare, and recreation activities in accordance with DoDI 8550.01.

4.5. DODIN CLOUD SERVICES CONNECTIONS. Connections to a CSO, both internal and external to the DODIN, will be implemented in accordance with the DoD Cloud Computing Security Requirements Guide, the DCCPG (until integrated with the DCPG), and applicable DoD policy.

a. Before connecting to the DODIN, CSOs must have a DoD provisional authorization issued in accordance with the Cloud Computing Security Requirements Guide.

b. DoD Components will only use CSOs, and DoD systems supported by the CSOs, that were granted an ATO or interim authorization to test by their AO.

c. DODIN access to CSOs that have a DoD provisional authorization will be updated in DISA's integrated joint tracking and management repository.

d. CSOs hosting DoD information connected to DoD networks and systems that do not comply with the DCCPG (until integrated with the DCPG) will require DoD CIO approval.

SECTION 5: RESOURCE MANAGEMENT

5.1. DISN FUNDING AND COST RECOVERY.

a. The DISN Infrastructure Service will function as the cost recovery methodology and concept employed by DISA to bill customers for the operation, production, and overhead costs of the DISN and DISN services, and to recoup reimbursement for DISN costs, common services (e.g., dial tone), DoD Component enclave interconnection services to the DISN (physical and virtual), DISN computing services telecommunications infrastructure costs, and other capabilities identified in the annually published DISN rates. Additions or deletions of DISN-IS cost components are approved by the DoD CIO and subsequently the USD(C)/CFO. These funds will be recouped in accordance with DoD 7000.14-R.

b. The DISN uses a combination of expense and investment funds to provide Enterprise solutions and infrastructure life-cycle management.

c. The DISN is responsible for resourcing all equipment that directly provides connectivity, routing, and enterprise services between DISN operating locations and the DISN PE router on an installation. The DISN does not fund similar components for the DoD Component enclave.

d. DISN carrier ethernet private IP and MPLS services and access circuits are provided on a reimbursable basis by either the user or DISA.

e. Tenants are allowed to use the DISN Infrastructure Service in accordance with the MOA established with the installation host for that location.

5.2. DOD-COMPONENT ENCLAVE FUNDING AND COST RECOVERY.

a. The installation host for a base, camp, post, or station is responsible for resourcing DoD Component enclave telecommunications infrastructure, as defined in this issuance, between the tenants and the DISN infrastructure to provide a local common IT transport backbone.

(1) This does not include special tenant requirements or equipment.

(2) Formal agreements (e.g., MOAs, HTSAs, interservice support agreements) must specify the cost recovery mechanisms to support special missions and equipment.

b. The installation host will ensure that DoD Component enclave capabilities are planned, operated, maintained, managed, and improved effectively and efficiently for end-to-end interoperability through technical refresh, technical evolution, and sustainment in accordance with DoDI 4000.19 and the Deputy Secretary of Defense Joint Basing Implementation Guidance.

c. The installation host will bill tenants in accordance with DoD 7000.14-R and the approved formal agreement between the parties.

GLOSSARY

G.1. ACRONYMS.

ADN	area distribution node
AO	authorizing official
ATO	authorization to operate
BAN	base area network
CAP	cloud access point
CCRI	command cyber readiness inspection
CD	cross domain
CDC	core data center
CDRUSCYBERCOM	Commander, U.S. Cyber Command
CJCS	Chairman of the Joint Chiefs of Staff
CNSSI	Committee on National Security Systems Instruction
COMSEC	communications security
CSO	cloud service offering
CSP	cloud service provider
DCO-IDM	defensive cyberspace operations – internal defense measures
DCCPG	DISN Cloud Connection Process Guide
DCPG	DISN Connection Process Guide
DIA	Defense Intelligence Agency
DISN	Defense Information Systems Network
DISA	Defense Information Systems Agency
DoD CIO	DoD Chief Information Officer
DoDD	DoD directive
DoDI	DoD instruction
DODIN	Department of Defense Information Network
DSS	Defense Security Service
EPPC	enterprise perimeter protection capability
HTSA	host tenant support agreement
IAP	internet access point
IC	Intelligence Community
IG	installation gateway
IP	internet protocol
IPN	installation processing node
ISN	installation service node
IT	information technology
JFHQ-DODIN	Joint Force Headquarters DODIN

JIE	Joint Information Environment
JWICS	Joint Worldwide Intelligence Communication System
MOA	memorandum of agreement
MGW	mobility gateway
MPE	Mission Partner Environment
MPGW	mission partner gateway
MPLS	Multi-Protocol Layer Switching
NIPRNet	Non-classified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
RMF	risk management framework
SATCOM	satellite communication
SIPRNet	Secret Internet Protocol Router Network
TCN	tactical communication node
TR	telecommunication room
UC	unified capabilities
USCYBERCOM	U.S. Cyber Command
USD(C)/CFO	Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense
USD(I)	Under Secretary of Defense for Intelligence
USD(P)	Under Secretary of Defense for Policy
VoIP	Voice over Internet Protocol
VPN	virtual private network

G.2. DEFINITIONS. Unless otherwise noted, these terms and their definitions are for the purpose of this issuance.

ADN. A capability that supports extending voice, video, and data services from the ISN to distant locations on the BAN and is comprised of back-up and tertiary power, heating, ventilation, and air conditioning, building surge protector assemblies, main cross connect blocks, equipment support frames, rectifiers, repeaters, and the IT equipment necessary to extend networks and systems to the end user buildings the ADN services.

ATO. Defined in Committee on National Security Systems Instruction (CNSSI) 4009.

AO. Defined in CNSSI 4009.

backside connection. An indirect physical extension of DODIN services, across a separate and distinct intermediate accreditation boundary, to a third party. For example, a connection between a Combatant Command, Military Service, or Defense Agency enclave and a defense Contractor

enclave or another network (e.g., Internet, SDREN) that does not traverse the DISN but can provide a connection to the DISN through the Combatant Command, Military Service, or Defense Agency enclave. A connection to another DoD Component system or network established consistent with DoD policy and Security Technical Implementation Guides is not considered a backside connection.

CDC. The most robust and capable DoD data centers designated as the mandatory providers of all Enterprise-wide computing and storage capabilities. They are marked by the following key attributes: Initially operated by DISA, but in the future may also include commercially operated CDCs; standardized operations, processes, and governance across all CDCs; fixed or permanent facilities meeting Uptime Institute Standards Tier III standards and later Tier IV standards; high bandwidth connections to the DISN core backbone; hosting of Enterprise net-centric applications and core Enterprise services and applications; regional content staging; Enterprise-scale computing and storage; scalable space, power, and infrastructure; meet all exemplar data center criteria.

certification. Defined in CNSSI 4009.

civil-military partners. Defined in DoDI 8220.02.

cloud. Defined in NIST Special Publication 800-145. Also known as cloud computing.

CAP. A capability that provides access to the commercial cloud, interface translations necessary for CSO compatibility, and supports boundary cyber defense by protecting the DISN from the commercial cloud.

Common Mission Network Transport. A network transport facilitated by the DISN backbone enabling Combatant Commands an alternative method to share releasable classified and unclassified information with mission partners by providing a dedicated transport service for allied, coalition, interagency, and bilateral Community of Interest networks.

COMSEC. Defined in CNSSI 4009.

connection. A link between computer networks employing wire, fiber-optic cable, radio frequency signal, or virtual network technologies, such as a VPN and generic routing encapsulation.

connectivity. Anything physically or logically connected to a customer's or user's enclave or network.

cross domain solution. Defined in CNSSI 4009.

CSO. The actual infrastructure as a service, platform as a service, or software as a service solution available from a CSP.

CSP. Any or all DoD or non-DoD entities that offer one or more cloud services in one or more deployment models. A CSP might leverage or outsource services of other organizations and other CSPs (e.g., placing certain servers or equipment in third party facilities such as data

centers, carrier hotels or collocation facilities, and internet network access points. CSPs offering Software as a Service may leverage one or more third party CSPs (e.g., for Infrastructure as a Service or Platform as a Service) to build out a capability or offering.

cybersecurity. Defined in the DoD Dictionary of Military and Associated Terms.

cybersecurity and cybersecurity-enabled products. Products that have any mechanism providing for the availability of systems, ensuring the integrity and confidentiality of information, or ensuring the authentication and non-repudiation of parties in electronic transactions.

cybersecurity service. Defined in DoDI 8530.01.

cyberspace. Defined in the DoD Dictionary of Military and Associated Terms.

defense contractor. Defined in DoDI 3020.41.

Defense Switched Network. Defined in the DoD Dictionary of Military and Associated Terms.

directive authority for cyberspace operations. Defined in DoDI 8530.01.

disconnect. Indicates the use of a service (e.g., connection or circuit) is to be suspended but the service path remains intact and the user continues to be billed for the service.

discontinue. Indicates a service (e.g., connection or circuit) is to be ended permanently and the user is no longer billed for the service.

DISN. DoD's enterprise capability of DoD-owned and -leased telecommunications and computing subsystems, networks, and capabilities, centrally managed and configured by DISA, to provide an integrated network with cybersecurity, telecommunication, computing, and application services and capabilities (e.g., voice, video, teleconferencing, computing, imagery, satellite, and data services) for all DoD activities and their authorized mission partners. This term and its definition are proposed for inclusion in the next edition of the DoD Dictionary of Military and Associated Terms.

DoD Component-provided DODIN transport. The segment of DODIN transport under the operational direction and management control of the DoD Components. DoD Component – provided DISN transport includes:

Sustaining base telecommunications infrastructures (e.g., bases, camps, posts, and stations and enclaves) to support strategic and fixed environment user requirements within the DoD Component base infrastructures. Management control and operational direction is provided by the owning DoD Component.

Deployed telecommunications infrastructures supporting joint task forces and/or combined task forces. Management control and operational direction is provided by the owning Combatant Command and subordinate Military Service component.

Mobile and/or transportable telecommunications facilities and assets organic to the DoD Components (unless specifically designated as components of the DISN).

DoD information. Defined in DoDD 5230.09.

DODIN. Defined in the DoD Dictionary of Military and Associated Terms.

DODIN transport. The composite of all DoD-owned and leased telecommunications subsystems and networks comprised of facilities, personnel, and material. It is divided into two segments: the DISN and the DoD Component enclave transport.

DODIN Transport Optimization Plan. Documented actions to eliminate legacy circuits and transport technologies and transition to existing IP bandwidth or readily available commercial IP network transport (e.g., carrier ethernet private IP or MPLS services) and cloud services to connect sites to the DISN. The objective of these actions is to enhance the performance of DoD network infrastructures (e.g., IP-based) and aggressively eliminate costly legacy network technologies (e.g., time-division multiplexing), associated transport infrastructure, and circuits.

enclave. Defined in CNSSI 4009.

Enterprise CD Service. Defined in DoDI 8540.01.

Enterprise Directory Service. A suite of products and services, comprised of enterprise provisioning services, directory services, synchronization services, and enterprise white pages. The Enterprise Directory Service supports people discovery by securely providing DoD Enterprise identity and contact attributes across the DoD community. Source identity information is retrieved from DISA's Global Directory Services and Defense Manpower Data Center's Person Data Repository, a key component of the Defense Enrollment and Eligibility Reporting System.

enterprise services. Defined in DoDD 8000.01.

external network. Defined in CNSSI 4009.

geographically separated unit. A unit separated beyond a reasonable commuting distance from its supporting Combatant Command, Military Service, or Defense Agency and does not physically reside on a main installation that belongs to another service/entity.

Global Content Delivery Service. An Enterprise-level service, consisting of a globally distributed computing platform of servers deployed across the DISN, to accelerate delivery and improve reliability of web applications through the efficient use of limited network bandwidth.

IAP. Approved connections from the internet to the NIPRNet that provides common enterprise security services for all DoD Components, including Enterprise Email Security Gateway, access controls, network firewall protections, intrusion and detection sensors, and other transport layer security services.

IG. The required localized equipment necessary to connect a B/P/C/S, CDC, or Installation Processing Node to the DISN Core. Equipment may include routers, switches, or UC firewalls.

incident. Defined in CNSSI 4009.

information service. Defined in Public Law 104-104.

information transport. To convey information from one location to another.

installation. Defined in DoDI 1015.11.

interconnection. See "connection."

internet. Defined in CNSSI 4009.

IP. Defined in CNSSI 4009.

IPN. A fixed DoD data center serving a single DoD installation and local area (installations physically or logically behind the network boundary) with local services that cannot be (technically or economically) provided from a CDC. There will be no more than one IPN per DoD installation, but each IPN may have multiple enclaves to accommodate unique installation needs (e.g., joint bases).

ISN. The required localized equipment necessary to provide the minimum basic functionality to an installation should it become disconnected from the enterprise. ISN is typically comprised of distribution frames and associated panels, equipment that delivers common services (e.g., dial tone, voicemail, conference bridging) to all users on the installation, and the equipment necessary to operate and maintain the telecommunications infrastructure. There is no application hosting or data processing in an ISN. Potential services include read only active directory servers, domain name service servers, Assured Compliance Assessment Solution servers, host-based security system servers, and print servers. ISNs may also host UC capabilities that must remain on the installation to enable emergency services even when the connection to the DODIN is interrupted.

IT. Defined in CNSSI 4009.

JIE. A secure joint information environment, comprised 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.

JRSS. A suite of equipment that performs firewall functions, intrusion detection and prevention, enterprise management, virtual routing and forwarding, and provides a host of network security capabilities for the NIPRNet and SIPRNet.

life-cycle. Defined in the DoD Dictionary of Military and Associated Terms.

MGW. A capability to provide secure ingress to the DODIN for users of mobile devices and direct cellular carrier connections to DoD-approved mobility users.

minimize. A condition wherein nonessential voice, video, and data traffic is drastically reduced or removed through available means, user or technical, to ensure that critical information connected with an actual or simulated emergency, surge, or crisis must not be delayed and meet DoD mission requirements. This term and its definition are proposed for inclusion in the next edition of the DoD Dictionary of Military and Associated Terms.

mission partners. Defined in DoDD 8000.01.

MOA. Defined in DoDI 4000.19.

national security system (NSS). Defined in CNSSI 4009.

network. Defined in CNSSI 4009.

network connection. The physical and electrical boundary between two separate communication systems.

outside plant. Fiber-optic or copper cable installed between buildings.

platform IT system. Defined in DoDI 8510.01.

risk management. Defined in CNSSI 4009.

SATCOM gateways. A capability consisting of a ground facility, SATCOM security gateway and SATCOM terminal components that allows interconnections to the DODIN via satellite. These interconnections include satellite-to-terrestrial interfaces to DODIN and legacy C4I systems to support deployed forces and joint task forces.

security domain. Defined in CNSSI 4009.

service. A set of capabilities enabled by a provider for consumers. For example, cloud services, video services, voice services, cybersecurity services, and messaging.

SIPRNet. Defined in the DoD Dictionary of Military and Associated Terms.

sponsor. Defined in CNSSI 4009.

system. Defined in CNSSI 4009.

TCN. A capability for tactical users to communicate locally, access services from a tactical processing node, or access data or services from the JIE, including the DISN. TCNs support various means of communications, including SATCOM, protected, fiber, beyond line of site, and line of site, to including Wi-Fi and cellular.

telecommunications. Defined in CNSSI 4009.

telecommunications infrastructure. A collection of interconnected telecommunications components, such as switches, routers, hubs, modems, media converters, distribution frames and cross-connect devices, cabling, telecommunications controllers, key distribution centers,

technical control devices, etc. used to provide transmission services for IT capabilities (voice, video, and/or data communications) over a combination of DoD and commercial media (terrestrial, wireless, or radio frequency).

TR. An enclosed space for housing telecommunications equipment, cable terminations, and cross-connect cabling that is the recognized location of the horizontal cross-connect in a facility.

Unified Capabilities (UC). Defined in DoDI 8100.04.

VPN. Defined in CNSSI 4009.

vulnerability assessment. Defined in CNSSI 4009.

REFERENCES

Chairman of the Joint Chiefs of Staff Instruction 3170.01, Joint Capabilities Integration and Development System (JCIDS), January 23, 2015

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

Defense Information Systems Agency, "Defense Information Systems Network (DISN) Connection Process Guide (DCPG)," current edition

Defense Information Systems Agency, "Defense Information Systems Network (DISN) Cloud Connection Process Guide (DCCPG)," current edition (until integrated with the DCPG)

Defense Intelligence Agency Instruction 8550.002, "Joint Worldwide Intelligence Communications Systems Connection Approval," May 2, 2014

Deputy Secretary of Defense Memorandum, "Establishment of the Office of the Under Secretary of Defense for Research Engineering and the Office of the Under Secretary of Defense for Acquisition and Sustainment," July 13, 2018

DISA Circular 310-55-9, "Base Level Support for the DISN," April 4, 2014

DISA Circular 310-130-2, "Management Threshold (MT) and Performance Objectives (PO)," October 1, 2012

DoD 5200.08-R, "Physical Security Program," April 9, 2007, as amended

DoD 5220.22-M, "National Industrial Security Program Operating Manual," February 28, 2006, as amended

DoD 7000.14-R,"Department of Defense Financial Management Regulations (FMRs)," date varies by volume

DoD Chief Information Officer, "Defense Information Systems Network (DISN) Global Information Grid (GIG) Flag Panel Charter," April 2012, as amended

DoD Directive 2010.9, "Acquisition and Cross-Cutting Agreements," April 28, 2003, as amended

DoD Directive 3020.44, "Defense Crisis Management," June 4, 2007

DoD Directive 3025.13, "Employment of DoD Capabilities in Support of the U.S. Secret Service (USSS), Department of Homeland Security (DHS)," October 8, 2010

DoD Directive 3025.18, "Defense Support of Civil Authorities (DSCA)," December 2, 2010

DoD Directive 5000.02, "Operation of the Defense Acquisition System," January 7, 2015

DoD Directive 5105.19, "Defense Information Systems Agency (DISA)," July 25, 2006

DoD Directive 5118.03, "Under Secretary of Defense (Comptroller)/Chief Financial Officer, Department of Defense (USD(C)/CFO)," April 20, 2012

DoD Directive 5134.01, "Under Secretary of Defense for Acquisition, Technology, and Logistics (USD(AT&L))," December 9, 2005

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

DoD Directive 5230.09, "Clearance of DoD Information for Public Release," August 22, 2008, as amended

DoD Directive 5400.11, "DoD Privacy Program," October 29, 2014

DoD Directive 5500.07, "Standards of Conduct," November 29, 2007

DoD Directive 5530.3, "International Agreements," June 11, 1987, as amended

DoD Directive 7045.14, "The Planning, Programming, Budgeting, and Execution (PPBE) Process," January 25, 2013

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

DoD Directive 8100.02, "Use of Commercial Wireless Devices, Services, and Technologies in the Department of Defense (DoD) Global Information Grid (GIG)," April 14, 2004, as amended

DoD Instruction 1015.10, "Military Morale, Welfare, and Recreation (MWR) Programs," July 6, 2009, as amended

DoD Instruction 1015.11, "Lodging Policy," October 6, 2006

DoD Instruction 1015.15, "Establishment, Management, and Control of Nonappropriated Fund Instrumentalities and Financial Management of Supporting Resources," October 31, 2007, as amended

DoD Instruction 3000.05, "Stability Operations," September 16, 2009

DoD Instruction 3003.01, "DoD Support to Civil Search and Rescue (SAR)." September 26, 2011

DoD Instruction 3020.41, "Operational Contract Support (OCS)," December 20, 2011

DoD Instruction 3025.19, "Procedures for Sharing Information with and Providing Support to the U.S. Secret Service (USSS), Department of Homeland Security (DHS)," November 29, 2011, as amended

DoD Instruction 4000.19, "Support Agreements," April 25, 2013

DoD Instruction 5000.02, "Operation of the Defense Acquisition System," January 7, 2015, as amended

DoD Instruction 5000.64, "Accountability and Management of DoD Equipment and Other Accountable Property," May 19, 2011

DoD Instruction 5200.44, "Protection of Mission Critical Functions to Achieve Trusted Systems and Networks (TSN)," November 5, 2012, as amended

DoD Instruction 5220.22, "National Industrial Security Program (NISP)," March 18, 2011

DoD Instruction 5410.19, "Public Affairs Community Relations Policy Implementation," November 13, 2001

DoD Instruction 5535.10, "Coordination of DoD Efforts to Identify, Evaluate, and Transfer DoD Technology Items, Equipment, and Services to Federal, State, and Local First Responders," November 24, 2009

DoD Instruction 6055.17, "DoD Installation Emergency Management (IEM) Program," February 13, 2017

DoD Instruction 8100.04, "DoD Unified Capabilities (UC)," December 9, 2010

DoD Instruction 8110.01, "Mission Partner Environment (MPE) Information Sharing Capability Implementation for the DoD," November 25, 2014

DoD Instruction 8220.02, "Information and Communications Technology (ICT) Capabilities for Support of Stabilization and Reconstruction, Disaster Relief, and Humanitarian and Civic Assistance Operations," April 30, 2009

DoD Instruction 8320.02, "Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 5, 2013

DoD Instruction 8320.07, "Implementing the Sharing Data, Information, and Information Technology (IT) Services in the Department of Defense," August 3, 2015

DoD Instruction 8330.01, "Interoperability of Information Technology (IT), Including National Security Systems (NSS)," May 21, 2014

DoD Instruction 8410.02, "Netops for the Global Information Grid (GIG)," December 19, 2008

DoD Instruction 8410.03, "Network Management (NM)," August 29, 2012

DoD Instruction 8420.01, "Commercial Wireless Local-Area Network (WLAN) Devices, Systems, and Technologies," November 3, 2009

DoD Instruction 8440.01, "DoD Information Technology (IT) Service Management (ITSM)," December 24, 2015

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

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

DoD Instruction 8523.01, "Communications Security (COMSEC)," April 22, 2008

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

DoD Instruction 8540.01, "Cross Domain (CD) Policy," May 8, 2015

DoD Instruction 8550.01, "DoD Internet Services and Internet-Based Capabilities,"

September 11, 2012

DoD Instruction 8551.01, "Ports, Protocols, and Services Management (PPSM)," May 28, 2014

DoD Regulation 7000.14-R,"Department of Defense Financial Management Regulations (FMRS)," Various

Memorandum of Agreement between the Departments of Defense and Homeland Security, January 19, 2017

National Institute of Science and Technology Special Publication 800-47, "Security Guide for Interconnecting Information Technology Systems," August 2002

National Institute of Science and Technology Special Publication 800-97, "Establishing Wireless Robust Security Networks: A Guide to IEEE 802.11i," February 2007

National Telecommunications & Information Administration, "Manual of Regulations and Procedures for Federal Radio Frequency Management," September 2015

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

Public Law 104-104, "Telecommunications Act of 1996," February 8, 1996

Under Secretary of Defense for Intelligence Memorandum, "Directive-Type Memorandum (DTM) 09-012, 'Interim Policy Guidance for DoD Physical Access Control'," December 8, 2009

Unified Command Plan, April 6, 2011, as amended

Unified Facilities Criteria 3-580-01, "Telecommunications Interior Infrastructure Planning and Design," June 1, 2016

U.S. Code, Title 10

U.S. Code, Title 31, Section 1535

U.S. Security Authority for North Atlantic Treaty Organization Affairs Instruction 1-07, "Implementation of NATO Security Requirements," 2007